

**IMPLEMENTACIÓN DE UN MODELO PARA EL SEGUIMIENTO Y CONTROL
DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS
ASIGNADOS EN LOS DIFERENTES SISTEMAS DE INFORMACIÓN DE
COLJUEGOS**

**RODRIGO ALARCÓN ÁVILA
IVÁN DARÍO LEÓN ALFONSO**

**UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2016**

**IMPLEMENTACIÓN DE UN MODELO PARA EL SEGUIMIENTO Y CONTROL
DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS
ASIGNADOS EN LOS DIFERENTES SISTEMAS DE INFORMACIÓN DE
COLJUEGOS**

**RODRIGO ALARCÓN ÁVILA
IVÁN DARÍO LEÓN ALFONSO**

**Proyecto de Grado para optar al título
de Especialista en Seguridad Informática**

**Tutores: Lorena Ocampo Correa
Álvaro Escobar Escobar**

**UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2016**

Nota de aceptación:

Firma Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C. 18 de octubre de 2016

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

Lorena Ocampo Correa, tutor del proyecto

Álvaro Escobar Escobar, Director Especialización en Seguridad Informática

A la Universidad Piloto de Colombia

A todas aquellas personas que de una u otra forma han colaborado en la elaboración de este proyecto.

CONTENIDO

	pág.
INTRODUCCIÓN	22
1. ASPECTOS DE LA INVESTIGACIÓN	23
1.1 JUSTIFICACIÓN	23
1.2 FORMULACIÓN DEL PROBLEMA	24
1.2.1 Pregunta de investigación.	25
2. OBJETIVOS	26
2.1 OBJETIVO GENERAL	26
2.2 OBJETIVOS ESPECÍFICOS	26
3. MARCO TEÓRICO	27
3.1 FUNDAMENTOS	27
3.2 MECANISMOS PARA EL ASEGURAMIENTO DE LA INFORMACIÓN	28
3.2.1 Identificación	28
3.2.2 Autenticación	28
3.2.3 Autorización	29
3.2.4 Auditoría	29
3.3 GESTOR DE IDENTIDADES Y CONTROL DE ACCESO	30
3.4 SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS.	32

4. ANÁLISIS DE LA SITUACIÓN ACTUAL	34
4.1 POLITICA CORPORATIVA DE GOBIERNO DE IDENTIDAD	34
4.2 LINEAMIENTOS Y PROCEDIMIENTOS PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS.	34
4.3 INFORMACIÓN DE ENTRADA PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS, EN LA ACTUALIDAD.	35
4.4 MODELO PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS.	38
4.5 HERRAMIENTAS INFORMÁTICAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS.	38
4.6 CONSULTAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS.	39
5. DISEÑO E IMPLEMENTACIÓN DEL MODELO	40
5.1 ESTRUCTURA DEL MODELO IMPLEMENTADO	40
5.2 NUEVAS POLÍTICAS CORPORATIVAS DE GOBIERNO DE IDENTIDAD IMPLEMENTADAS	42
5.3 NUEVOS LINEAMIENTOS Y PROCEDIMIENTOS PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS, IMPLEMENTADAS EN COLJUEGOS.	47
5.3.1 Políticas corporativas de gobierno de identidad implementadas	47
5.3.2 Actualización del procedimiento de gestión de cuentas de usuarios de Coljuegos	47
5.4 INFORMACIÓN CONSIDERADA EN EL MODELO PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS.	53
5.4.1 Estructura de información de los funcionarios.	55
5.4.2 Estructura de información de las novedades de personal	57

5.4.3 Formatos para solicitar roles y permisos por cada una de las aplicaciones de Coljuegos	58
5.5 HERRAMIENTAS INFORMÁTICAS CONSIDERADAS PARA EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS.	63
5.6 CONSULTAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS.	67
6. AVANCES OBTENIDOS EN LA APLICACIÓN DEL MODELO	73
6.1 APLICACIÓN DE LAS NUEVAS POLÍTICAS CORPORATIVAS DE GOBIERNO DE IDENTIDAD, LINEAMIENTOS Y PROCEDIMIENTOS	73
6.2 USO DE HERRAMIENTAS INFORMÁTICAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE ROLES Y PRIVILEGIOS ASIGNADOS A CADA USUARIO EN COLJUEGOS.	77
6.3 AUDITORIAS Y CONSULTAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS.	84
7. CONCLUSIONES	85
BIBLIOGRAFÍA	87
ANEXOS	92

LISTA DE FIGURAS

	pág.
Figura 1. Estructura del modelo implementado	40
Figura 2. Instructivo de gestión de cuentas de usuario	48
Figura 3. Estructura de la información y sus interrelaciones para el seguimiento y control de la administración de usuarios, roles y privilegios.	53
Figura 4. Registro de roles y perfiles	58
Figura 5. Formato para el ingreso de roles y perfiles SIPLAFT	59
Figura 6. Formato para el ingreso de roles y perfiles SIITO	60
Figura 7. Formato para el ingreso de roles y perfiles ORFEO	61
Figura 8. Formato para el ingreso de roles y perfiles MET-SCLM	62
Figura 9. Categorías creadas en MANTIS para la administración de usuarios, roles y privilegios.	66
Figura 10. Solicitud para ingreso de personal en la gestión de cuentas de usuarios, roles y privilegios MANTIS.	67
Figura 11. Muestra de algunos usuarios	70
Figura 12. Ingreso de personal 2016 MANTIS.	75
Figura 13. Muestra de solicitudes atendidas en el año 2016 sobre gestión de usuarios, roles y privilegios	76
Figura 14. MANTIS como herramienta para el seguimiento y control de usuarios, roles y privilegios.	78
Figura 15. ACCESS como herramienta para el seguimiento y control de usuarios, roles y privilegios.	78

Figura 16. SQL ORACLE como herramienta para el seguimiento y control de usuarios, roles y privilegios.	80
Figura 17. SQL SERVER parte A, como herramienta para el seguimiento y control de usuarios, roles y privilegios.	80
Figura 18. SQL SERVER parte B, como herramienta para el seguimiento y control de usuarios, roles y privilegios.	82
Figura 19. EXCEL como herramienta para el seguimiento y control de usuarios, roles y privilegios.	83

LISTA DE TABLAS

pág.

Tabla 1. Resumen solicitudes atendidas en el año 2016 sobre gestión de usuarios, roles y privilegios.

74

LISTA DE CUADROS

	pág.
Cuadro 1. Controles y actividades implementadas de la ISO 27001	43
Cuadro 2. Atributos de la estructura funcionarios:	56
Cuadro 3. Estructura de funcionarios	57
Cuadro 4. Muestra de algunos usuarios	68
Cuadro 5. Roles ORFEO	92
Cuadro 6. Permisos ORFEO	93
Cuadro 7 Roles SIICOL.	97
Cuadro 8. Módulos SIICOL.	98
Cuadro 9. Permisos SIICOL.	102
Cuadro 10. Roles, módulos y permisos SIICOL	103
Cuadro 11. Proyectos MANTIS.	151
Cuadro 12. Roles MANTIS.	156
Cuadro 13. Permisos MANTIS.	157
Cuadro 14. Roles SIPLAFT	157
Cuadro 15. Permisos SIPLAFT.	158
Cuadro 16. Roles MET-SCLM	158
Cuadro 17. Permisos MET.SCLM.	159
Cuadro 18. Roles SIITO	160
Cuadro 19. Permisos SIITO	160

LISTA DE ANEXOS

	pág.
Anexo A. Roles y privilegios de las aplicaciones	92

GLOSARIO

AUDITORÍA. Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base a ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones.¹

AUTENTICACIÓN. Definimos la Autenticación como la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.²

AUTONOMÍA ADMINISTRATIVA. Libertad que se concede para dirigir, según normas y órganos propios, todos los asuntos concernientes a su administración.³

AUTORIZACIÓN. Es el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización. El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.⁴

CANAL PQRD. Proceso mediante el cual una compañía hace la gestión de las peticiones, quejas, reclamos y denuncias que hacen los clientes. En términos generales, por tratarse de un proceso, implica las connotaciones de tiempo, espacio requeridos, es decir contempla personas, tecnologías y recursos en general, para garantizar respuestas efectivas.⁵

COLJUEGOS. Empresa Industrial y Comercial del Estado Administradora del Monopolio Rentístico de los Juegos de Suerte y Azar. Entidad descentralizada del orden nacional, vinculada al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y patrimonio independiente.

¹ MUÑOZ RAZO, Carlos. Auditoría en sistemas computacionales. Primera edición. México: Prentice hall. 2002. 796p

²RECURSOSTIC. Mecanismos básicos de seguridad. Recuperado el 02 de octubre de 2016 de: <http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=2>

³ UNIVERSO JUS. Definición de Autonomía Administrativa. Recuperado el 23 de agosto de 2016 de: universojus.com/definición/autonomía-administrativa

⁴RECURSOSTIC. Mecanismos básicos de seguridad. Recuperado el 02 de octubre de 2016 de: <http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=2>

⁵ MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. ¿Qué es canal PQRD?: Recuperado el 23 de agosto de 2016 de: www.mintic.gov.co

Coljuegos, tiene como objeto la explotación, administración, operación y expedición de reglamentos de los juegos que hagan parte del monopolio rentístico sobre los juegos de suerte y azar que por disposición legal no sean atribuidos a otra entidad.⁶

CONFIDENCIALIDAD. Propiedad de la información que determina que esté disponible a personas autorizadas.⁷

CONTINUIDAD DE NEGOCIO. Aunque existe una diferencia significativa, cada organización establece las medidas necesarias y proporcionales a sus necesidades para garantizar su continuidad en caso de desastre. Si hablamos del ámbito tecnológico, por ejemplo, mientras que una gran organización puede requerir el despliegue de un centro de respaldo alternativo, tanto de comunicaciones, sistemas como servidores en una ubicación remota, en otros casos podría ser más óptimo realizar copias de seguridad en la nube, primando el rendimiento frente al coste.⁸

CUENTAS HUÉRFANAS. Cuentas que no tienen un propietario. Pueden ser fácilmente utilizadas para conseguir acceso no autorizado a recursos e información confidencial de la compañía. La identificación y eliminación de dichas cuentas supone una reducción drástica de los niveles de vulnerabilidad digital de cualquier organización.⁹

DIRECTORIOS VIRTUALES. Un directorio virtual es un directorio del servidor que no está dentro del directorio de publicación habitual, es decir, un directorio que no depende de C:\inetpub\wwwroot pero que sí se puede acceder a través del servidor web como si estuviera dentro de dicho directorio.¹⁰

DISPONIBILIDAD. Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.¹¹

EMPRESA DESCENTRALIZADA. Integran igualmente la rama ejecutiva y se encargan de cumplir funciones que corresponden al estado, gracias a la descentralización de funciones, tienen autonomía para desarrollar sus actividades

⁶ COLJUEGOS. Coljuegos. Recuperado el 02 de agosto de 2016 de <http://www.coljuegos.gov.co/loader.php?IServicio=Glosario&letra=C>

⁷ MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Confidencialidad. Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

⁸ INCIBE. Plan de Contingencia y Continuidad de Negocio. Recuperado el 02 de octubre de 2016 de: <https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio>

⁹ IBM. Cuentas huérfanas. Recuperado el 02 de octubre de 2016 de: http://www.ibm.com/support/knowledgecenter/es/SSTFWV_5.1.0/com.ibm.itim.doc/ref/ref_ic_reportspack_orphan_account.html

¹⁰ MICROSOFT. ¿Qué son directorios virtuales? Recuperado el 23 de agosto de 2016 de: <https://support.microsoft.com/es-co/kb/142853>

¹¹ MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Disponibilidad. Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

y gozan de las prerrogativas que les concede la ley que las crea. Su objeto principal es el ejercicio de funciones administrativas, la prestación de servicios públicos o la realización de actividades industriales o comerciales con personería jurídica, autonomía administrativa y patrimonio propio.¹²

GESTIÓN DE IDENTIDADES. La gestión de identidad (gestión de ID) se ocupa de la identificación de individuos en un sistema, así como de controlar su acceso a los recursos dentro de ese sistema mediante la asociación de derechos de usuario y restricciones conforme a la identidad establecida. Tiene como objetivo el control de la información, así como de los usuarios en los sistemas de información: autenticación, nivel de acceso a la información y acciones autorizadas son algunas de sus atribuciones.¹³

GESTIÓN DE ROLES. Control estricto de qué información se quiere dar acceso y cuál es el grado de permisos que queremos asignar a cada empleado.¹⁴

GESTIÓN DE USUARIOS. La gestión de usuarios es la actividad referida a la creación y mantenimiento de cuentas de usuarios, así como la de asignación de recurso y seguridad en los accesos de la red.¹⁵

MESA DE AYUDA. La Mesa de Ayuda y Soporte es un equipo de trabajo, punto de contacto entre los usuarios de la empresa y las tecnologías estándares adoptadas por la misma, y cuyo objetivo principal será responder de una manera oportuna, eficiente y con alta calidad a las peticiones que dichos usuarios realicen, en relación a los diversos aspectos de la Tecnología de la Información.¹⁶

IAM- INTEGRATED ACCESS MANAGEMENT. Gestión de Identidad y Acceso (IAM) es un servicio que le permite administrar usuarios y permisos de usuario dentro de un sistema de información más o menos complejo. Con una solución de IAM, se puede administrar de forma centralizada los usuarios, credenciales de seguridad como claves de acceso y permisos que controlan, el cual los usuarios pueden acceder a todos y sólo los recursos de su competencia.¹⁷

¹² UDEA. Las Entidades Descentralizadas. Recuperado el 02 de octubre de 2016 de: http://docencia.udea.edu.co/derecho/constitucion/eje_conform_entidades_desc.html

¹³ ID MANAGEMENT. Gestión de identidades. Recuperado el 23 de agosto de 2016 de: Search.datacenter.techtarget.com/es/definicion/Gestion-de-identidades-ID-management

¹⁴ WORDPRESS. Definición de gestión de roles. Recuperado el 23 de agosto de 2016 de: <https://ecoleccion.wordpress.com/category/moodle/gestion-de-roles/>

¹⁵ GOOGLE DOCS. Gestión de Usuarios. Recuperado el 02 de octubre de 2016 de: https://docs.google.com/document/d/1wyg6NbMoiFEg6lZZ_POBZFx7ly3fx3xPcpQ8olcMXiQ/edit

¹⁶ EL MUNDO DE LAS TICS. Gestión de mesa de ayuda. Recuperado el 02 de octubre de 2016 de: http://www.elmundodelastics.net/2008/10/la-funcin-de-una-mesa-de-ayuda-en-los.html#.V_Vwfo_hCUk

¹⁷ INTEGRATE ACCESS MANAGEMENT. ¿Qué es gestión de Identidad y Acceso (IAM)? Recuperado el 23 de agosto de 2016 de: www.gartner.com/it/identity-and-access-management-iam

IDENTIFICACIÓN. Se denomina Identificación al momento en que el usuario se da a conocer en el sistema.¹⁸

INGENIERÍA DE ROLES. La ingeniería de roles es el proceso de definición de roles, permisos y asignación de permisos para cada rol en la organización. Esto es esencialmente un proceso de ingeniería de requerimientos de roles. La ingeniería de roles es el primer paso hacia la implementación de un sistema de accesos basado en roles.¹⁹

INTEGRIDAD. Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.²⁰

ISO 27001. Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.²¹

ITRC. Unidad Administrativa Especial Agencia del Inspector General de Tributos, Rentas y Contribuciones parafiscales.²²

LDAP. Son las siglas de *Lightweight Directory Access Protocol* (en español Protocolo Ligero/Simplificado de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.²³

LÍDERES FUNCIONALES. Son los responsables de coordinar en conjunto con el cliente la definición de las necesidades existentes en la organización y transformarlas en requerimientos. Este rol funge como cliente final ante el equipo técnico.²⁴

¹⁸SEGU-INFO. Seguridad Lógica – Identificación y Autenticación. Recuperado el 02 de octubre de 2016 de: <http://www.segu-info.com.ar/logica/identificacion.htm>

¹⁹EVOLUTION-IT. Ingeniería de roles. Recuperado el 02 de octubre de 2016 de: <http://www.evolution-it.com.co/portafolio/gestion-de-la-seguridad/ingenieria-de-roles.html>

²⁰ MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Integridad. Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

²¹ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO 27001. Recuperado el 23 de agosto de 2016 de: www.iso.gov.co

²²COLJUEGOS. Sabes que es el ITRC. Recuperado el 02 de octubre de 2016 de: <file:///C:/Users/sistemas01/Downloads/ITRC.pdf>

²³INSTITUTO DE TECNOLOGIA DE MASSACHUSETTS. Capítulo 13. Protocolo ligero de acceso a directorios (LDAP). Recuperado el 02 de octubre de 2016 de: web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ldap.html

²⁴DIALNET. Qué son líderes funcionales. Recuperado el 23 de agosto de 2016 de: <https://dialnet.unirioja.es/descarga/articulo/4895442.pdf>

MANTIS. Software que constituye una solución completa para gestionar tareas en un equipo de trabajo. Es una aplicación *Open Source* realizada con php y mysql que destaca por su facilidad y flexibilidad de instalar y configurar. Esta aplicación se utiliza para testear soluciones, hacer un registro histórico de alteraciones y gestionar equipos remotamente.²⁵

META-DIRECTORIOS. Software utilizado para replicar datos entre diferentes fuentes, aunque estas fuentes no tengan nada que ver entre sí. Podría llamarse un conector de bases de datos de diferentes fuentes o fabricantes.²⁶

MET-SCLM. Es un sistema de conexión en línea de un grupo de Máquinas Electrónicas Tragamonedas (MET). Las máquinas son conectadas con una interfaz a través de un protocolo de comunicaciones y por medio de una conexión segura a un Servidor Concentrador del Operador (SCO) local o remoto.²⁷

MODELO. Los modelos son constructos diseñados por un observador que persigue identificar y mensurar relaciones sistémicas complejas. Todo sistema real tiene la posibilidad de ser representado en más de un modelo. La decisión, en este punto, depende tanto de los objetivos del modelador como de su capacidad para distinguir las relaciones relevantes con relación a tales objetivos. La esencia de la modelística sistémica es la simplificación. El meta-modelo sistémico más conocido es el esquema input-output.²⁸

NO REPUDIO. El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente.²⁹

OBJETO. Se define a un objeto como "una entidad tangible que muestra alguna conducta bien definida". Un objeto "es cualquier cosa, real o abstracta, acerca de la cual almacenamos datos y los métodos que controlan dichos datos".³⁰

²⁵MANTISBT. Mantis. Recuperado el 02 de octubre de 2016 de <https://www.mantisbt.org/>

²⁶ WORDPRESS. Metadirectorios. Recuperado el 23 de agosto de 2016 de <https://buscadores.espanol.wordpress.com/tag/metadirectorios>

²⁷COLJUEGOS; Requerimientos Técnicos Sistema Conexión en Línea Máquinas Electrónicas Tragamonedas SCLM. Recuperado el 02 de octubre de 2016 de: www.coljuegos.gov.co/descargar.php?idFile=216213

²⁸ UNIVERSIDAD DE CHILE. Introducción a los conceptos básicos de la Teoría General de Sistemas. Recuperado el 02 de octubre de 2016 de www.facso.uchile.cl/publicaciones/moebio/03/frprinci.htm

²⁹ UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Definición de No repudio. Recuperado el 23 de agosto de 2016 en: redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServNoRepudio.php

³⁰PROFESORES.FI. ¿Que es objeto? Recuperado el 02 de agosto de 2016 en: http://profesores.fi-b.unam.mx/carlos/aydoo/conceptos_oo.html

ORFEO. Orfeo es un sistema de Gestión Documental y de procesos desarrollado inicialmente por la Superintendencia de Servicios Públicos Domiciliarios (SSPD) en Colombia, licenciado como software libre bajo licencia GNU/GPL para compartir el conocimiento y mantener la creación colectiva.³¹

PERMISO. Acciones autorizadas que un sujeto puede realizar sobre un objeto.³²

PERSONERÍA JURÍDICA. La personería jurídica o personalidad jurídica es el reconocimiento a un ser humano, una organización, una empresa u otro tipo de entidad para asumir una actividad o una obligación que produce una plena responsabilidad desde la mirada jurídica, tanto frente a sí mismo como respecto a otros.³³

POLÍTICA CORPORATIVA DE GOBIERNO DE IDENTIDAD. Normas internas de las empresas, principalmente, privadas que siguen las directrices marcadas por la dirección. Habitualmente, para crearlas es necesario un análisis y estudio de la misma empresa, el contexto en que está ubicada y su competencia. Teniendo en cuenta estos y otros factores, se crean las dichas políticas corporativas. El objetivo de las cuales es mejorar el rendimiento, la calidad y la jerarquía de dicha empresa.³⁴

POLÍTICA SGSI. Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.³⁵

PRIVILEGIOS. Permiso para realizar una acción, asignable a un usuario o un rol.³⁶

ROLES. Conjunto de privilegios, asignables a un usuario o un rol.³⁷

³¹ ORFEOLIBRE. Orfeo sistema de gestión documental. Recuperado el 02 de octubre de 2016 en: <http://www.orfeolibre.org/portal/>

³²DC.UBA. Definición de permiso. Recuperado el 02 de octubre de 2016 en: http://www-2.dc.uba.ar/materias/seginf/material/Clase02-Unidad2_vf.pdf

³³ GERENCIE.COM. Qué es personería jurídica. Recuperado el 23 de agosto de 2016 en: gerencie.com/persona-juridica.html

³⁴ PROSPERIDAD SOCIAL. política corporativa de gobierno de identidad Recuperado el 23 de agosto de 2016 en: [www.prosperidadsocial.gov.co/.../Manual%20de%20Identidad % 20 Corporativa%20Pr...](http://www.prosperidadsocial.gov.co/.../Manual%20de%20Identidad%20Corporativa%20Pr...)

³⁵ISO 27000. Política y objetivos de seguridad. Recuperado el 02 de octubre de 2016 en: http://www.iso27000.es/download/doc_sgsi_all.pdf

³⁶REDCIENTIFICA. Conceptos de gestión de privilegios y recursos. Recuperado el 02 de octubre de 2016 en: <http://www.redcientifica.com/oracle/c0004p0004.html>

³⁷REDCIENTIFICA. Conceptos de gestión de privilegios y recursos. Recuperado el 02 de octubre de 2016 en: <http://www.redcientifica.com/oracle/c0004p0004.html>

SEGURIDAD DE LA INFORMACIÓN. Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.³⁸

SERVICIO DE DIRECTORIOS (SD). Es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores y sobre los recursos de red que permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red.³⁹

SIICOL. Sistema Integrado de Información Coljuegos.⁴⁰

SIPLAFT. Sistema de Prevención y Control de Lavado de Activos y Financiación del Terrorismo. Es un sistema que se materializa en un documento que contiene los compromisos adquiridos por el operador autorizado de juegos de suerte y azar con el Estado colombiano, de adoptar un sistema de prevención y control del lavado de activos y financiación del terrorismo en su empresa, con el fin de evitar que la misma sea usada para fines delictivos.⁴¹

SISTEMA DE INFORMACIÓN. Conjunto total de procedimientos, operaciones, funciones y difusión de datos o información en una organización.⁴²

SUJETO. Proceso informático que actúa en lugar del usuario.⁴³

SÚPER USUARIO. Cuenta de usuario que posee todos los derechos en todos los modos (mono o multiusuario). Normalmente esta es la cuenta de administrador.⁴⁴

TIC. Aplicación de las Tecnologías de la Información y las Comunicaciones -TIC en apoyo a medidas nacionales para la superación de la pobreza, el aumento de la competitividad y la superación de problemáticas en diferentes poblaciones, sectores y territorios.⁴⁵

³⁸BOGOTATURISMO. Norma Técnica Colombiana NTC-ISO/IEC 27001. Recuperado el 02 de octubre de 2016 en: <http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf>

³⁹ REDIRIS. Servicios de directorios. Recuperado el 23 de agosto de 2016 en: <https://www.rediris.es/ldap/doc/ldap-intro.pdf>

⁴⁰ COLJUEGOS. Sistema Integrado de Información de Coljuegos. Recuperado el 23 de agosto de 2016 en: www.coljuegos.gov.co/descargar.php?idFile=215916

⁴¹ COLJUEGOS. ¿Qué es Siplaft? Recuperado el 23 de agosto de 2016 en: www.coljuegos.gov.co/publicaciones/300493

⁴² GERENCIE. Sistemas de información. Recuperado el 23 de agosto de 2016 en: www.gerencie.com/sistemas-de-información

⁴³ ISEGORIA. ¿Qué es sujeto? Recuperado el 23 de agosto de 2016 en: isegoria.revistas.csic.es/index.php/isegoria/article/viewFile/95/95

⁴⁴ SUPERSU. ¿Qué es súper usuario? Recuperado el 23 de agosto de 2016 en: supersu.uptodown.com/Android

⁴⁵ MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. TIC para el desarrollo. Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

USUARIO. Persona o máquina delegada por un cliente para utilizar los servicios y/o facilidades de una red de telecomunicaciones. En el contexto de los servicios de telecomunicación: un ser humano que utiliza un servicio. En un contexto técnico: un ser humano, una entidad o un proceso. Nota - Un usuario no será necesariamente un abonado a un servicio de telecomunicación.⁴⁶

UTM. La gestión unificada de amenazas, que comúnmente se abrevia como UTM, es un término de seguridad de la información que se refiere a una sola solución de seguridad, y por lo general un único producto de seguridad, que ofrece varias funciones de seguridad en un solo punto en la red. Un producto UTM generalmente incluye funciones como antivirus, *anti-spyware*, *anti-spam*, *firewall* de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas.⁴⁷

⁴⁶ MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Usuario (UIT-T Rec M.60 (93)). Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

⁴⁷ UNIVERSIDAD TÉCNICA DE MANAUBI. ¿Qué es UTM? Recuperado el 23 de agosto de 2016 en: www.utm.edu.ec/

RESUMEN

En la construcción del presente modelo para el seguimiento y control de la administración de usuarios, roles y permisos asignados en los diferentes sistemas de información, se desarrollaron las siguientes tareas: 1) construcción de políticas al respecto, 2) actualización del procedimiento de gestión de cuentas de usuarios, 3) implementación en el software de mesa de ayuda, el proyecto denominado “Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos” para facilitar y dejar la traza de las solicitudes que realizan los Jefes de Oficina, Vicepresidentes y Gerentes de Coljuegos, quienes son los que deben solicitar la creación, modificación, activación, inactivación, de usuarios, roles, perfiles y permisos para el acceso a la información de los sistemas de información, 4) actualización del procedimiento del área de Capital Humano para que informen a través del software de mesa de ayuda, las novedades de administración de personal (ingresos, traslados, egresos, vacaciones, licencias maternidad/paternidad, comisiones, incapacidades, licencias No remuneradas, etc.), con el fin se tomen las acciones correspondientes a la gestión de cuentas de usuario, 5) canalización hacia los líderes funcionales de cada sistema, las autorizaciones de asignación de usuarios, roles y privilegios, 6) registro en tablas de la información requerida para llevar el control y seguimiento de las novedades de usuarios, roles y privilegios, 7) mediante el uso de herramientas informáticas (Excel, Access, y SQL), realizar el control y seguimiento de roles y privilegios asignados a cada funcionario en cada aplicación y 8) realización del cruce de la información autorizada versus la asignada para producir los informes de auditoría correspondientes.

Con la implementación de este modelo se ha podido evidenciar: 1) mejoramiento de la confidencialidad e integridad de la información en Coljuegos, 2) aumento de la confianza de los usuarios evitando vulnerabilidades derivadas de accesos indebidos por parte de usuarios, 3) mejor seguimiento, control y traza de la administración de usuarios, roles y privilegios asignados a cada sistema de información y 4) facilidad para el desarrollo de auditorías al respecto.

INTRODUCCIÓN

Las empresas enfrentan retos cada vez más exigentes para lograr ser competitivas y rentables, por lo que requieren optimizar los procesos de negocio y mejorar la seguridad de la información que las soporta. El uso de múltiples sistemas de información, aplicaciones y estándares facilita la proliferación de diversas identidades digitales para clientes, empleados y socios del negocio.

La gestión de identidades y control de acceso (IAM- *Integrated Access Management*), es una solución que permite realizar la gestión del ciclo de vida de las identidades de los usuarios y controlar el acceso a los diferentes recursos, con el fin de mitigar riesgos, reducir costos y permitir que el negocio evolucione de manera segura y flexible, pero debido al costo elevado en el mercado de este tipo de software y a los recortes presupuestales de Coljuegos, no ha sido posible adquirir e implementar una herramienta de este tipo, por lo cual se ha visto en la necesidad de mejorar los controles de acceso a las diferentes aplicaciones de otra manera.

El objetivo de este trabajo consiste en la implementación de un modelo para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información, el cual contribuye a mejorar la confidencialidad e integridad de la información en Coljuegos.

1. ASPECTOS DE LA INVESTIGACIÓN

1.1 JUSTIFICACIÓN

Debido a los recortes constantes de recursos presupuestales, Coljuegos no ha logrado adquirir un software para la administración centralizada de identidades, el cual facilitaría la asignación y control de acceso a los sistemas de información e instalaciones de Coljuegos, por lo que ha tenido que recurrir a la administración manual de cada uno de ellos, con las dificultades que esto conlleva. Sin embargo, no por ello se puede descuidar las responsabilidades de una buena administración del control de acceso a los diferentes recursos e información.

Con el transcurso de los años, se han implementado más sistemas de información en Coljuegos, así mismo se han incrementado las actividades para la gestión de usuarios en cada una de éstas, lo cual induce a un seguimiento y control deficiente en la asignación de usuarios, roles y privilegios. Esta implementación para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos, mejora esta situación y logra los siguientes beneficios:

- Disposición de unas políticas corporativas de gobierno para el seguimiento y control de usuarios, roles y privilegios.
- Disposición de lineamientos generales y procedimientos para el seguimiento y control de usuarios, roles y privilegios.
- Coadyuva en la aplicación correcta de los roles y privilegios a cada usuario y aplicación.
- Facilita la auditoría sobre el acceso que tienen los usuarios a sus recursos y aplicaciones, permitiendo proteger la información confidencial, de usuarios no autorizados.
- Contribuye a la confidencialidad, integridad y disponibilidad de la información.
- Aumenta la seguridad de la información y confianza de los usuarios evitando vulnerabilidades derivadas de accesos indebidos por parte de usuarios con cuentas huérfanas o bien de accesos indebidos a sistemas por parte de usuarios que ya no deberían poder hacerlo por haber cambiado su posición o puesto.
- Cumplimiento de la legislación colombiana avalado con informes y cuadros de mando, relativo al control de acceso (autenticación y nivel de autorización), auditoría de los procesos de alta, baja y modificación de usuarios de los sistemas,

establecimiento de políticas corporativas de seguridad (contraseñas, aprobaciones de procesos).

1.2 FORMULACIÓN DEL PROBLEMA

En el mes de febrero del año 2015, el ITRC (Unidad Administrativa Especial Agencia del Inspector General de Tributos, Rentas y Contribuciones parafiscales), en su informe de auditoría presentado a Coljuegos, evidenció que no se garantiza la administración segura de Roles y privilegios en los sistemas de información, exponiendo a Coljuegos al riesgo de fallas en la confidencialidad, Integridad y disponibilidad de la información, debido a que no se cuenta con lineamientos e instrumentos para crear, actualizar, inactivar y hacer seguimiento a los roles y privilegios asignados. Indica que, de acuerdo con los lineamientos de seguridad de la información establecidos por el Ministerio de las Tecnologías de la Información y Comunicaciones, la identificación de usuarios debe ser única para cada usuario y debe garantizar el no repudio de las transacciones y de las responsabilidades, al igual que se debe restringir y controlar la asignación y uso de privilegios.

Actualmente Coljuegos cuenta por cada sistema de información y aplicativo, con una persona para la creación de usuarios y asignación de roles y privilegios, lo cual ocasiona fallas como las siguientes:

- Se crean varias cuentas para un mismo usuario. Así, por ejemplo, al usuario Pedro Pérez, se le pudo haber creado en la aplicación 1 con la cuenta Pérez y en la aplicación 2 con la cuenta Pedro Pérez. Así mismo, la cuenta creada en el directorio activo para ingresar a la red de Coljuegos también pudo haberse creado con un nombre diferente.
- Claves o *password* diferentes para el ingreso a cada aplicación.
- Ausencia de depuración de usuarios y privilegios.
- Cuentas activas de personal que ya no se encuentran en la entidad.
- Cuentas con más privilegios de los que debería tener.
- Cuentas activas en algunos sistemas de información que no se utilizan o no deberían utilizarse debido al traslado de personal entre dependencias.

La pérdida de seguridad en la información afecta directamente a la actividad de una empresa pudiendo poner en riesgo la supervivencia de la misma. Así mismo, la dirección de Coljuegos tiene la responsabilidad de cumplir las reglas de controles internos y garantizar el cumplimiento de las obligaciones de nuevas regulaciones

tales como la privacidad y seguridad de la información contemplada en el decreto 2573 de diciembre de 2014, el cual comprende las acciones tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.

La gestión inadecuada de la administración de usuarios, roles y privilegios, puede encadenar una pérdida de calidad de los datos: La información de usuarios es inconsistente entre los diferentes sistemas, es decir, que un usuario dispone de privilegios acordes a su puesto o perfil dentro de un sistema en un determinado momento, y sin embargo mantiene privilegios erróneos en otros sistemas derivados de un puesto o perfil que quizá tuvo en otro momento y que no fueron modificados al cambiar sus circunstancias. Esta mala calidad de datos tiene impacto sobre el servicio.

1.2.1 Pregunta de investigación. ¿De qué forma se puede hacer un mejor seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar un modelo para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información, el cual contribuya a mejorar la confidencialidad e integridad de la información en Coljuegos.

2.2 OBJETIVOS ESPECÍFICOS

- Definir unas políticas corporativas de gobierno identidad para el seguimiento y control de la administración de usuarios, roles y privilegios.
- Definir los lineamientos y procedimientos generales para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos.
- Identificar y definir los datos de entrada para lograr el seguimiento y control de la administración de usuarios, roles y privilegios asignados a cada sistema de información.
- Diseñar el modelo de seguimiento y control para lograr el seguimiento y control de la administración de usuarios, roles y privilegios asignados a los sistemas de información.
- Usar herramientas informáticas que faciliten el seguimiento y control de roles y privilegios asignados a cada usuario en Coljuegos.
- Generar consultas que faciliten el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos.

3. MARCO TEÓRICO

3.1 FUNDAMENTOS

Con el decreto 4142 del 3 de noviembre de 2011, el gobierno colombiano, crea la Empresa Industrial y Comercial del Estado Administradora del Monopolio Rentístico de los Juegos de Suerte y Azar – Coljuegos, la cual es una empresa descentralizada del orden nacional, vinculada al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y patrimonio independiente, cuyo objeto es la explotación, administración, operación y expedición de reglamentos de los juegos que hagan parte del monopolio rentístico sobre los juegos de suerte y azar que por disposición legal no sean atribuidos a otra entidad.

El modelo para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información, se implementó desde la Oficina de Tecnologías de la Información, Oficina que depende directamente de la Presidencia de Coljuegos. Dicho modelo contribuye a mejorar la seguridad de la información en toda la entidad.

La importancia de la seguridad en los sistemas informáticos de una empresa es parte fundamental para su desempeño. Hoy en día el conocimiento es parte esencial de la naturaleza de las empresas, en otras palabras, lo que en su gran mayoría buscan las empresas. Por tanto, la información que procesan las organizaciones debe encontrarse digitalizada y protegida dentro de un marco de seguridad.

Para generar un marco de seguridad en sus recursos y sistemas informáticos, la empresa engloba sus acciones al respecto en tres aspectos:

- Manejo del riesgo
- Continuidad de negocio
- Seguridad de sistemas informáticos

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información (sistemas de información, sistemas de archivo, bases de datos, acceso a internet), buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Al trabajar en el entorno de la seguridad de la información debemos tener en cuenta la siguiente terminología:

- **Usuario:** se refiere a las personas que utilizan la computadora.
- **Sujeto:** proceso informático que actúa en lugar del usuario.
- **Objeto:** es cualquier recurso informático que esté disponible para su acceso.
- **Operación:** es un proceso que es invocado por un sujeto.
- **Permiso:** es la autorización para acceder al recurso o sistema.

3.2 MECANISMOS PARA EL ASEGURAMIENTO DE LA INFORMACIÓN

Existen ocho mecanismos básicos funcionales para el aseguramiento de la información digital: identificación, autenticación, autorización, no rechazo, integridad, auditoría, privacidad y disponibilidad. Éste trabajo trata del seguimiento y control a los roles y privilegios asignados a los usuarios en los diferentes sistemas de información, los cuales están más relacionados con la identificación, autenticación, autorización y auditoría. A continuación, damos una pequeña explicación de éstos últimos conceptos.

3.2.1 Identificación. Sirve para que los usuarios se den a conocer en el sistema, esto normalmente se conoce como la cuenta o *login* del usuario. Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

3.2.2 Autenticación. Verifica que los usuarios que se hayan identificado correspondan a usuarios válidos dentro del sistema. El proceso de autenticación es quizás la pieza inicial y fundamental del control de la seguridad de la información. Es en esencia lo que permite indicar que una persona que dice que es, en realidad lo sea.

Todo proceso de autenticación involucra dos categorías:

- Una cadena de identificación lógica es asignada a un sujeto y,
- Algún tipo de información es relacionada con ese usuario para validar que sea la persona que dice que es.

Las categorías mencionadas provienen de la información correspondiente de la persona:

- **Lo que la entidad conoce o lo que uno sabe:** conocimiento de la persona. Ejemplo: la contraseña.
- **Lo que la entidad tiene o lo que uno tiene:** en posesión de la persona. Ejemplo: tarjeta.
- **Lo que la entidad es o por lo que uno es:** biometría del sujeto. Ejemplo: huella digital

3.2.3 Autorización. Este proceso tiene como objetivo la protección de los recursos computacionales de accesos que no estén autorizados. En este proceso se lleva el control de acceso a los recursos y sistemas informáticos según el flujo de trabajo que corresponda. Lo anterior se realiza con base a políticas de seguridad por lo cual solo se permite el acceso según las autorizaciones asignadas a cada usuario.

Los modernos mecanismos de control de acceso están basados en el concepto de monitoreo por referencia, el cual interviene en cada acceso que realiza un sujeto a un recurso de conformidad con una política de seguridad que lo regula.

En el monitoreo por referencia se distinguen dos factores importantes:

- Realización del control de acceso.
- La decisión de control de acceso.

3.2.4 Auditoría. Consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización.

El incumplimiento de los requerimientos de auditoría puede dar como resultado problemas en los niveles de seguridad de la información, lo que puede llevar a incidentes de seguridad y en algunos casos a pérdidas económicas y de imagen.

3.3 GESTOR DE IDENTIDADES Y CONTROL DE ACCESO

El presente trabajo está relacionado con los gestores de identidades y control de acceso (IAM), toda vez que el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de una organización hace parte de ellos, por lo que es importante tener una visión general de este tipo de herramientas.

Un IAM se compone de un conjunto de procesos de negocio, tecnologías, infraestructura y políticas que permite realizar la gestión de las identidades de usuario y controlar el acceso de éstas a los diferentes recursos organizacionales. Involucra diferentes procesos y áreas de la organización, desde la alta gerencia hasta las áreas de soporte y apoyo, cuya implementación y buenos resultados depende de la disposición y grado de compromiso que demuestre cada uno de los diferentes actores.

Debido a la cantidad de accesos que son necesarios crear por la cantidad de aplicaciones, a las permanentes novedades de personal tales como ingresos, retiros, salida a vacaciones, incapacidades, etc., cada vez es más complicado implementar controles que garanticen que los usuarios son los que deberían estar activos en cada una de las aplicaciones, o que las credenciales de inicio sean iguales en todos los sistemas. Lo anterior deja entrever que las identidades tienen un ciclo de vida que es necesario administrar.

Por lo general todo usuario que ingresa a un sistema tiene asignados unos roles y privilegios que también son necesarios administrar. Un rol y privilegio mal asignado conlleva a accesos no autorizados a la información y a los recursos protegidos, ocasionando incidentes en donde se compromete la confidencialidad e integridad de éstos. Lo que se busca con un IAM es una solución que permita la asignación efectiva de roles y privilegios, dependiendo de las funciones que desempeña cada usuario dentro de la organización.

Entre algunos beneficios que se pueden lograr al implementar un IAM, encontramos:

- Proteger los datos de la organización contra robo y falta de confidencialidad e integridad de éstos.
- Cada usuario tiene los accesos a la información y recursos necesarios para el desempeño de su cargo.
- Cumplimiento de las regulaciones existentes sobre protección de datos.

- Reducción de costos administrativo, toda vez que por lo regular se requiere de un responsable de asignar a los usuarios, los roles y perfiles correspondientes a cada sistema de información y aplicación.
- Como la gestión de usuarios/identidades es centralizada, la productividad mejora debido a que la asignación de roles y privilegios de cada usuario de las aplicaciones es mucho más rápida que tener que realizar las asignaciones por cada una de las aplicaciones.
- Consistencia de los datos relacionados con la identidad de los usuarios, porque ya no será necesario tenerlos por cada una de las aplicaciones, sino que éstos se encuentran en un repositorio central, normalmente en el directorio activo, de donde serán utilizados por las diferentes aplicaciones. Por lo mismo, es más fácil actualizar estos datos cuando sea requerido, es decir, no se requiere actualizar los datos en cada una de las aplicaciones, sino que con que se actualice en el repositorio central es suficiente.

Así como hay ventajas también se pueden considerar las siguientes desventajas o consideraciones a tener en cuenta cuando se implemente un IAM:

- Como cada usuario tiene un solo usuario y contraseña para ingresar a las diferentes aplicaciones o sistemas de información, será necesario utilizar sistemas robustos de autenticación, o sensibilizar permanentemente sobre el uso y cambio de contraseñas, para evitar posibles suplantaciones.
- Como la autenticación se hace sobre un repositorio central, será necesario que este repositorio sea de alta disponibilidad con mecanismos de replicación lo que implica mayores costos.
- Mayor tiempo y recursos en la ingeniería de roles para lograr una buena definición de acuerdo con los cargos y funciones. En ocasiones se requiere reestructuración de los procesos de la organización.
- El retorno de inversión de un proyecto de este tipo es a largo plazo.

Los componentes básicos de un IAM, puede resumirse en los siguientes:

- **Servicio de directorios:** el cual es administrado de forma central y contiene la información de los recursos que se compartirán con todas las aplicaciones.
- **Meta-directorios:** utilizados para recolectar y almacenar información de diversos servidores de directorios.

- **Directorios virtuales:** se encargan de crear una vista unificada de la información que procede de diferentes fuentes de la organización.
- **Gestión de identidades:** permite gobernar la creación, desarrollo y eliminación de las entidades y sus atributos dentro de un repositorio unificado de identidades. Se compone de diseño de identidad digital en término de las aplicaciones desplegadas dentro de la entidad. Los roles funcionales y unidad de negocio a la que pertenece hacen parte de este componente, al igual que los niveles de acceso hacia cada aplicación y los atributos de cada aplicación.
- **Gestión de Roles:** se administra el ciclo de vida de los roles asociados a los diferentes usuarios al interior de la organización, de acuerdo con las funciones y cargo desempeñado.
- **Gestión y control de acceso:** hace referencia al control, monitoreo y auditoria del acceso a los recursos ya sea por medio de los servicios ofrecidos en la red interna o externa de la organización. Se basa en las políticas de seguridad que emplean el uso de mecanismos de autenticación, autorización y confianza.

3.4 SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS

El seguimiento y control de la administración de usuarios, roles y privilegios, está relacionado con los controles de acceso basado en roles, los cuales permite asignar usuarios a roles y realizar un seguimiento de los permisos concedidos a cada rol. Las políticas de seguridad de la información permiten controlar la relación entre el control de acceso y la estructura de la organización.

Los roles asignados a cada usuario se basan en la función del cargo desempeñado por cada usuario. Puede usar los roles de autorización para autorizar el acceso, delegar privilegios administrativos o administrar la interacción con los recursos basados en equipos. Por ejemplo, puede definir un rol de Tesorero que incluya el derecho a autorizar gastos y a auditar transacciones contables.

Teniendo en cuenta lo que es un IAM y los controles de acceso basado en roles, el presente trabajo sólo abarca lo relacionado con el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información, deja de un lado toda la gestión de creación y modificación de usuarios, roles y privilegios en cada uno de los sistemas de información, esta labor la seguirá ejerciendo cada uno de los líderes funcionales de dichos sistemas con la herramientas o funcionalidades propias del sistema correspondiente.

El modelo implementado para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información, está relacionado con las labores propias de auditoría y contribuye a mejorar la confidencialidad e integridad de la información en Coljuegos.

4. ANÁLISIS DE LA SITUACIÓN ACTUAL

4.1 POLÍTICA CORPORATIVA DE GOBIERNO DE IDENTIDAD

Para la elaboración de unas políticas corporativas de gobierno de identidad para el seguimiento y control de la administración de usuarios, roles y privilegios, es necesario tener en cuenta las políticas actuales específicas de cada organización, de tal forma que las políticas a construir guarden concordancia y no vaya en contravía de las políticas generales, sino que por el contrario contribuya a la seguridad de la información.

Del análisis realizado, se concluye que Coljuegos no cuenta con unas políticas detalladas para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información.

Por lo anterior, se requiere se formulen unas políticas que respondan a la necesidad de Coljuegos, con el fin de establecer una cultura de calidad y seguridad que opere de forma confiable, con lo cual contribuya a la seguridad informática y se reduzcan los riesgos al respecto. Estas políticas tendrán por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones de todo el personal comprometido en el uso de los servicios informáticos proporcionados por la Oficina de Tecnologías de la Información, especialmente en el control y seguimiento de la administración de usuarios, roles y privilegios en los sistemas de información.

4.2 LINEAMIENTOS Y PROCEDIMIENTOS PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS

Analizados los diferentes lineamientos y procedimientos para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos, se encontró que existe el procedimiento denominado gestión de cuentas de usuarios, cuyo objetivo es el definir los pasos para crear y administrar las cuentas de usuario de los funcionarios de Coljuegos, las cuales permitirán el ingreso a los sistemas y herramientas de la entidad. Este documento se creó con el propósito de establecer y estandarizar los métodos, criterios, requisitos y responsabilidades de cada uno de los actores que intervienen en las actividades aquí descritas, pero no contiene lo relacionado con los usuarios, roles, perfiles y permisos que deben tener los funcionarios que acceden a los diferentes sistemas de información. En la asignación de éstos deben aplicarse el principio de mínimos privilegios y los lineamientos de seguridad de Coljuegos. Tampoco detalla las personas que autorizarían dichos accesos. Los

titulares de las Oficinas, las Vicepresidencias y Gerencias, deberían ser las personas adecuadas para autorizar dichos accesos.

Dentro de los proyectos y categorías contempladas en el software de mesa de ayuda, tampoco se encontró elementos que permitan a los diferentes funcionarios asignar incidencias relacionadas con la administración de usuarios, roles y perfiles para cada uno de los sistemas de información con que cuenta Coljuegos, por lo cual llevar un seguimiento y control de éstos no es posible y mucho menos llevar una traza de las solicitudes autorizadas, a quienes le fue asignada para que incluyera los usuarios, roles y privilegios en cada sistema de información o herramienta tecnológica.

Por lo anterior se hace necesario la actualización del procedimiento actual de gestión de cuentas de usuarios, así como también diseñar e implementar en la herramienta de mesa de ayuda, los elementos requeridos para facilitar a las personas que autorizan usuarios, roles y perfiles, para que coloquen sus diferentes solicitudes al respecto y de esta manera poder llevar un mejor control y seguimiento de los accesos.

4.3 INFORMACIÓN DE ENTRADA PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS, EN LA ACTUALIDAD

Los datos de entrada para el seguimiento y control de la administración de usuarios, roles y privilegios, está determinada por cada una de las aplicaciones. Para mayor detalle ver el anexo No A. Roles y perfiles de las aplicaciones.

Del análisis realizado se concluye que no es posible definir un estándar o unificación en la definición de roles y asignación de privilegios, puesto que cada aplicación en sí misma, tiene su propia finalidad y por consiguiente los roles, módulos y permisos son diferentes en cada una de ellas. Así por ejemplo para el caso del sistema Orfeo, la seguridad se administra asignándole al funcionario los roles y permisos, como se muestra a continuación.

Roles del sistema Orfeo:

- Administrador,
- Canal de Distribución,
- canal PQRD y
- Usuario Normal.

Permisos del sistema ORFEO:

- Digitalización de Documentos
- Modificaciones
- Impresión
- Solicitud de Anulaciones
- Administrador de Archivo
- Administrador del Sistema
- Usuario Reasigna
- Usuario Activo
- Usuario Nuevo
- Puede Archivar Documentos
- Creación de expedientes
- Remitentes / Terceros
- Tablas de Retención Documental
- Radicación Masiva
- Préstamo de Documentos
- Anulaciones
- Devoluciones de Correo
- Envíos de Correo
- Estadísticas

- Nivel de Seguridad
- Firma Digital
- Usuario Público
- Notificación de Resoluciones
- Trámite Respuesta Radicado
- Radicación Express
- (1) Salida
- (3) Interna
- (9) Históricos
- Reporte Radicación
- (2) Entrada
- (8) PQRD
- Puede borrar Anexos .tif
- Se autentica por medio de LDAP
- Puede Asignar Pre-radicado
- Puede Tipificar Anexos .tif
- Puede utilizar el editor de Flujos
- Resolución
- Autos
- Circulares

Para los sistemas SIPLAFT, MET-SCLM y SIITO, la seguridad de la información se realiza con roles y permisos diferentes a los de ORFEO. Para mayor detalle ver el anexo A. Roles y perfiles de las aplicaciones.

Para el caso del sistema SIICOL, a cada usuario se le asigna un rol, a su vez al rol se le asigna unos módulos y a los módulos se les asigna unos permisos. Para mayor detalle ver el anexo No A. Roles y perfiles de las aplicaciones.

4.4 MODELO PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS

El modelo actual para el seguimiento y control de la administración de usuarios, roles y privilegios, está totalmente delegada a través de los funcionarios líderes de cada aplicación. Existe un funcionario líder por cada una de las aplicaciones. Así, por ejemplo, la persona que asigna los usuarios, roles y privilegios en ORFEO es diferente de quién asigna los usuarios, roles y privilegios en el sistema SIICOL. Cada aplicación tiene un módulo de administración de usuarios que facilita la asignación de los correspondientes roles y permisos.

Actualmente, el seguimiento y control a los usuarios, roles y permisos asignados a los diferentes usuarios no es posible, todo depende de la buena fe de los líderes de cada aplicación, pues no se deja una traza de las autorizaciones correspondientes. La solicitud lo hace verbalmente y directamente el usuario al líder de cada aplicación.

4.5 HERRAMIENTAS INFORMÁTICAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS

Coljuegos no cuenta con software especializado que faciliten el seguimiento y control de las autorizaciones realizadas en la asignación de usuarios, roles y privilegios en las diferentes aplicaciones. Todo se hace de forma verbal directamente al funcionario líder de la aplicación y no se encuentra canalizado a través de los Jefes de Oficina, Vicepresidentes o Gerentes. El funcionario que considera necesitar de un permiso se lo solicita directamente al líder del aplicativo.

Aunque Coljuegos no cuenta con los recursos económicos para la compra de una herramienta especializada, si tiene herramientas informáticas como mantis, Access y Excel, las cuales se pueden aprovechar para realizar un mejor seguimiento y control en la asignación de cuentas, roles y permisos.

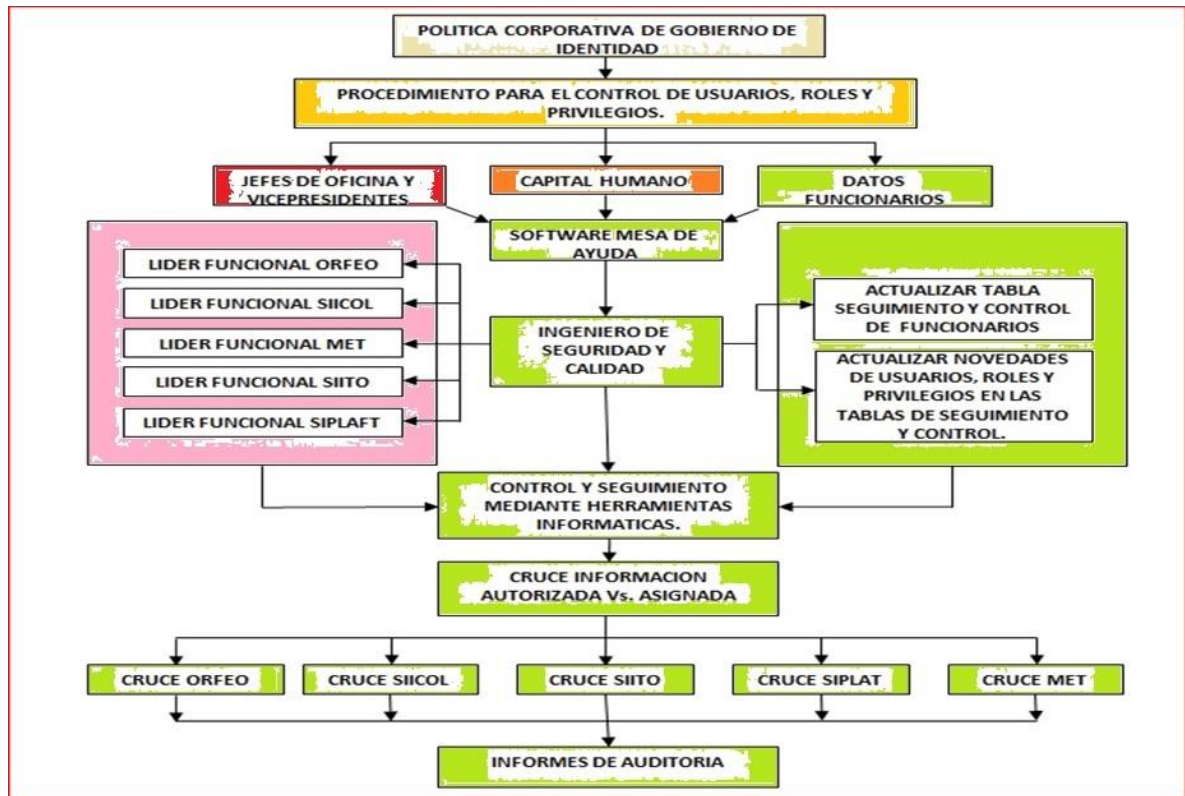
4.6 CONSULTAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS

Como actualmente, no se deja traza de la autorización previa de los roles y permisos asignados a cada funcionario, no es posible realizar un seguimiento y control adecuado de éstos. Lo que se realiza en estos momentos es simplemente desde cada sistema de información se consultan los diferentes roles y privilegios asignados a cada usuario. No hay nada con qué constatar, ni una persona que realice un seguimiento y control a éstos. No hay forma de verificar que los roles y permisos asignados sean los que se hayan autorizado.

5. DISEÑO E IMPLEMENTACIÓN DEL MODELO

5.1 ESTRUCTURA DEL MODELO IMPLEMENTADO

Figura 1. Estructura del modelo implementado



Fuente: autores

En el diseño del modelo para el seguimiento y control de la administración de usuarios, roles y permisos asignados en los diferentes sistemas de información, se consideraron los elementos y actividades que se muestran en la Figura 1, los cuales se describe a continuación:

- Primero, se construyeron las políticas corporativas de Gobierno de Identidad referentes al seguimiento y control de la administración de usuarios, roles y permisos, las cuales fueron implementadas y se encuentran relacionadas en la sección 5.2 de este documento.

- Segundo, fue necesario actualizar el procedimiento de gestión de cuentas de usuarios, el cual se muestra en la sección 5.3 de este documento debidamente actualizado.
- Tercero, se implementó en el software de mesa de ayuda, el proyecto denominado “Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos” para facilitar la labor de recibir solicitudes al respecto.
- Cuarto, los Jefes de Oficina, Vicepresidentes y Gerentes de Coljuegos, son los que deben solicitar a través del software de mesa de ayuda y proyecto “Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos”, la creación, modificación, activación, inactivación, de usuarios, roles, perfiles y permisos para el acceso a la información de los sistemas de información.
- Quinto, Capital Humano deberá a través del software de mesa de ayuda y proyecto “Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos”, informar las novedades de administración de personal (ingresos, traslados, egresos, vacaciones, licencias maternidad/paternidad, comisiones, licencias No remuneradas superiores a tres días e incapacidades superiores a tres días), con el fin se tomen las acciones correspondientes a la gestión de cuentas de usuario.
- Sexto, el Ingeniero de Seguridad y Calidad, canaliza hacia los líderes funcionales de cada sistema, las autorizaciones sobre la asignación de usuarios, roles y privilegios. Así mismo, actualiza con los datos recibidos, la tabla de funcionarios y registra las novedades de usuarios, roles y privilegios en las tablas de seguimiento y control correspondientes.
- Séptimo, los líderes funcionales de cada aplicación, asigna los roles y privilegios autorizados para cada una de las aplicaciones y que se encuentran relacionados en el anexo A de este documento.
- Octavo, el Ingeniero de Seguridad y Calidad, mediante el uso de herramientas informáticas (Excel y Access), lleva el control y seguimiento de roles y privilegios asignados a cada funcionario en cada aplicación.
- Noveno, periódicamente el ingeniero de seguridad y calidad realiza cruce de la información autorizada versus la asignada para producir los informes de auditoría correspondientes.

Siguiendo las anteriores actividades, se puede llevar un mejor control y seguimiento de los accesos a los sistemas de información en Coljuegos.

Es de anotar, que la traza de todas las solicitudes que se generan en el software de mesa de ayuda, a través del proyecto denominado “Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos”, coadyuva al control y seguimiento de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos.

5.2 NUEVAS POLÍTICAS CORPORATIVAS DE GOBIERNO DE IDENTIDAD IMPLEMENTADAS

Las siguientes Políticas Corporativas de Gobierno de Identidad, fueron incluidas dentro del documento de políticas de seguridad de la información de Coljuegos y fueron concebidas pensando en la privacidad de la información, lo cual se encuentra consagrado en las leyes 527 de 1999, la ley 1266 de 2008, la ley 1273 de 2009, la ley 1581 de 2012 y la norma ISO 27001. Estas normas, considera el uso eficiente de las Tecnologías de la Información y Comunicaciones y el Gobierno Electrónico, como una obligación que tiene el Estado, centrada en los ciudadanos y las personas naturales y jurídicas en general. La adecuada identificación electrónica como elemento transversal, coadyuva a la definición de políticas relacionadas con la gobernabilidad democrática, la transparencia, identidad e inclusión digital.

A continuación, se detallan las políticas implementadas en Coljuegos, las cuales se encuentran incluidas dentro del documento general de políticas de seguridad de la información:

- Para la implementación y mantenimiento de los sistemas de información y/o aplicaciones, el proceso TIC deberá contar con tres servidores independientes para los siguientes ambientes: desarrollo, pruebas y producción. En cada uno de ellos se debe restringir el acceso correspondiente y se debe dar acceso y permisos a las personas adecuadas de conformidad con el cargo que desempeñan.
- La creación, modificación, activación, inactivación, de usuarios, roles, perfiles y permisos para el acceso a la información de los sistemas de información, debe ser previamente autorizados por los Jefes de Oficina, Vicepresidentes y Gerentes de Coljuegos a través del software de mesa de ayuda.
- Se debe por lo menos una vez al año, depurar los usuarios, roles, perfiles y permisos para el acceso a la información de cada sistema de información.
- Se debe por lo menos una vez al año, realizar auditorías y monitoreo a los controles implementados para la gestión de acceso y privilegios asignados a los usuarios de los sistemas de información.

- Capital humano, informará al área de TIC y a través del software de mesa de ayuda, las novedades de administración de personal (ingresos, traslados, egresos, vacaciones, licencias maternidad/paternidad, comisiones, licencias no remuneradas superiores a tres días e incapacidades superiores a tres días), con el fin que se tomen las acciones correspondientes a la gestión de cuentas de usuario.
- El Ingeniero de Seguridad y Calidad, canaliza hacia los líderes funcionales de cada sistema, las autorizaciones sobre la asignación de usuarios, roles y privilegios.

Las anteriores políticas y los controles implementados de la ISO 27001, relacionados con la administración de usuarios, roles y privilegios, permiten mejorar la seguridad de la información en Coljuegos. En el cuadro 1 se muestran los controles seleccionados de la ISO 27001, el establecimiento de dicho control y las actividades implementadas al respecto en Coljuegos.

Cuadro 1. Controles y actividades implementadas de la ISO 27001

Control	Establecimiento del control	Actividades implementadas
Política de control del acceso	Se debe realizar la divulgación de la Política de Seguridad de la Información ítem "Política de Control de Acceso". Se recomienda mejorar las políticas de control de acceso mediante mejoras en las directivas de política de grupo del directorio activo. Ej.: Bloqueo automático, horarios de registro, etc.	La difusión de la política fue realizada por el Área de Comunicaciones y Recursos Humanos. Existe una política de bloqueo automático temporizado en tres minutos.
Registro de usuarios	La modificación del documento de Creación de cuentas de usuario por Documento Gestión de cuentas de usuario en donde se maneje la creación, modificación y eliminación de cuentas de usuario y en donde se contemple el retiro o bloqueo de derechos de acceso cuando es un retiro definitivo o en caso de bloqueo por vacaciones etc., definición de responsabilidades. Por medio del manejo del directorio activo se maneja id único para el funcionario. Este debe ser aprobado y puesto en uso.	Cada funcionario tiene un ID único en el directorio activo. El área de capital humano, informa a través de la mesa de ayuda cualquier novedad que ocurra con los empleados, tales como vacaciones, retiros, ingresos, calamidades, permisos, etc.

Continuación Cuadro 1. Controles y actividades implementadas de la ISO 27001

Control	Establecimiento del control	Actividades implementadas
Gestión de privilegios	<p>La modificación del documento de Creación de cuentas de usuario por Documento Gestión de cuentas de usuario en donde se maneja la creación, modificación y eliminación de cuentas de usuario y en donde se contempla el retiro o bloqueo de derechos de acceso cuando es un retiro definitivo o en caso de bloqueo por vacaciones etc., Por medio del manejo del directorio activo se maneja id único para el funcionario. Este debe ser aprobado y puesto en uso.</p> <p>Se debe establecer dentro de las auditorías internas la revisión de los privilegios de usuario dentro de todos los sistemas de la entidad.</p>	<p>Existe un procedimiento de creación de cuentas de usuario. La verificación de su cumplimiento es responsabilidad del ingeniero de calidad y seguridad.</p> <p>Se realizan auditorías internas que revisan los privilegios de usuario, dentro de todos los sistemas de la entidad.</p> <p>Cada jefe de área envía por el software de mesa de ayuda, la solicitud del rol y permisos que tendrá cada uno de sus funcionarios en cada una de las aplicaciones.</p>
Gestión de contraseñas para usuarios	<p>El control establece que todas las cuentas cuenten con un manejo de contraseñas seguro. Se debe limitar el uso de súper usuarios en casos que no se requieran y eliminar su uso en los usuarios personales de los funcionarios de TIC.</p>	<p>Por el directorio activo se exige el cambio de contraseña por mes, últimas 12 contraseñas recordadas, Ocho caracteres con complejidad.</p> <p>Las demás aplicaciones de la entidad se integrarán al uso de autenticación mediante el directorio activo.</p>
Uso de contraseñas	<p>Se debe realizar la divulgación de la Política de Seguridad de la Información en toda la entidad, para el manejo de contraseñas, realizar campañas de concientización sobre el manejo del uso de contraseñas</p>	<p>Se divulgó el documento con la sensibilización del alcance, políticas SI, política SGSI, reglamentación SGSI, estructura comité SGSI y metodología riesgos.</p> <p>Por el directorio activo se exige el cambio de contraseña por mes, últimas 12 contraseñas recordadas, Ocho caracteres con complejidad.</p>

Continuación Cuadro 1. Controles y actividades implementadas de la ISO 27001

Control	Establecimiento del control	Actividades implementadas
Procedimiento de ingreso seguro	El control establece limitar la cantidad de intentos permitidos de inicio de sesión. Se debería realizar monitoreo de las cantidades de intentos fallidos de registros de inicio. Se debería limitar los horarios de inicio de sesión.	La política de directorio activo para el bloqueo por ingresos fallidos está implementada.
Identificación y autenticación de usuarios.	El control establece realizar verificación de usuarios genéricos en aplicaciones o dispositivos de red, deben ser cambiados con ID único, o eliminados para poder llevar seguimiento de las acciones de los usuarios. Los perfiles de administrador no deben gestionar tareas regulares o normales, deben ser específicos.	Los usuarios internos se autentican por directorio activo. Los permisos de acceso a los usuarios son administrados centralmente en la intranet
Sistema de gestión de contraseñas	El control establece que para las aplicaciones se tengan un sistema de gestión de contraseñas con: ID único, permitir la selección y cambio de contraseñas, imponer selección de contraseña segura, imponer cambios de contraseña, forzar a cambiar las contraseñas temporales al inicio, conservar un registro de contraseñas previo para evitar su reutilización, almacenar los archivos de contraseñas separados de los datos de la aplicación y nunca en texto claro, proteger contraseñas en sistema cifrado. Fortalecer políticas de grupo de controlador de dominio	Mediante políticas de grupo sobre el controlador de dominio se establecen los requerimientos de contraseñas.
Tiempo de inactividad de la sesión	El control establece se evalúe para las aplicaciones el manejo de tiempo de inactividad en la sesión luego de inactividad para el cierre de sesiones de la aplicación y la red, y aún más cuando se tiene acceso desde un lugar externo. Fortalecer políticas de grupo de controlador de dominio.	El control de tiempos de inactividad para las aplicaciones, se coordina con los diferentes líderes de aplicaciones la implementación de dichos controles. En cuanto a las políticas de grupo para controlar los tiempos de actividad en la red, se implementa a través del directorio activo.

Continuación Cuadro 1. Controles y actividades implementadas de la ISO 27001

Control	Establecimiento del control	Actividades implementadas
Restricción del acceso a la información	Fortalecer políticas de grupo de controlador de dominio, en especial las opciones de Auditoría.	Se realizó el cambio de las políticas de directorio activo para incluir mejoras de los registros de Auditoría
Fuga de Información	El control establece que se debe considerar la limitación del riesgo sobre la fuga de información.	Se implementó un UTM.
Aprendizaje debido a los incidentes de seguridad de la información	El control establece crear un procedimiento de control de incidentes de seguridad de la información donde se identifique los eventos e Incidentes de seguridad de la información, canal de comunicación, responsabilidades para asegurar una respuesta rápida, eficaz y ordenada, aprendizaje del incidente y recolección de evidencia e implementarlo para toda la entidad.	Existe un procedimiento de gestión y reporte de incidentes.
Controles de auditoría de los sistemas de información	Se debe adicionar dentro del plan de Auditorías de la entidad, Auditorías internas sobre seguridad de la información en la entidad, y coordinar las condiciones para realizar Auditorías directamente a los sistemas de información de la entidad.	Aplicar los manuales de auditoría interna y acciones preventivas y correctivas del proceso de Evaluación y Mejora. Donde se incluye la Auditoría al SGSI
Protección de las herramientas de auditoría de los sistemas de información	Los controles implementados para la recolección de registros de auditoría deben ser revisados y auditados constantemente además de contar con restricciones de acceso especiales.	El ingeniero de calidad y seguridad es el responsable de definir los accesos a los registros de auditoría.
Acuerdos sobre confidencialidad.	Hacer revisión sobre la existencia de las cláusulas de confidencialidad en los contratos vigentes. La necesidad de los acuerdos debe ser valorada en conjunto con el área jurídica de acuerdo a los niveles de confidencialidad de la información a la cual va tener acceso.	Para los contratos suscritos por Coljuegos se incorporaron la cláusula de confidencialidad en las minutas de los contratos administrativos.

Continuación Cuadro 1. Controles y actividades implementadas de la ISO 27001

Control	Establecimiento del control	Actividades implementadas
Retiro de los derechos de acceso	El control sugiere que se establezca en el procedimiento de Gestión de Cuentas de usuario la eliminación de derechos de acceso inmediato. Esta solicitud debe ser tramitada por medio de la herramienta "Mantis" a aplicaciones e infraestructura tecnológica de Coljuegos. Realizar una verificación previa con el fin de evidenciar que se le han desactivado o eliminado todos los accesos permitidos, Adicionalmente cuando se presenta un cambio en el cargo se debe analizar que este usuario solo tenga acceso a lo requerido para el nuevo cargo y por lo tanto deshabilitar los demás accesos.	Existe un procedimiento de creación de cuentas de usuario. La verificación de su cumplimiento es responsabilidad del ingeniero de calidad y seguridad. El área de recursos humanos deberá informar de forma inmediata cualquier novedad mediante mantis al área de TI.

Fuente: autores



5.3 NUEVOS LINEAMIENTOS Y PROCEDIMIENTOS PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS, IMPLEMENTADAS EN COLJUEGOS

Los lineamientos y procedimientos generales diseñado para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos, se implementaron, así:

5.3.1 Políticas corporativas de gobierno de identidad implementadas. Las políticas corporativas de Gobierno de Identidad, se encuentran definidas anteriormente en la sección 5.2 de este documento.

5.3.2 Actualización del procedimiento de gestión de cuentas de usuarios de Coljuegos. El procedimiento debidamente actualizado de gestión de cuentas de usuarios de Coljuegos, se muestra en la Figura 2:

Figura 2. Instructivo de gestión de cuentas de usuario

 		GESTIÓN TIC'S GESTIÓN DE Cuentas DE USUARIO	Vigencia: 12/Ene/2016 Versión: 2 Código: TIC-IN-02
---	--	--	---

1. OBJETIVO

Crear y administrar las cuentas de usuario de los funcionarios de Coljuegos, las cuales permitirán el ingreso a los sistemas y herramientas de la entidad con los perfiles y privilegios respectivos, debe aplicarse el principio de mínimos privilegios y los lineamientos de seguridad de Coljuegos los cuales son autorizados por los titulares de las Oficinas, por las Vicepresidencias o Gerencias.

Este documento se crea con el propósito de establecer y estandarizar los métodos, criterios, requisitos y responsabilidades de cada uno de los actores que intervienen en las actividades aquí descritas.

2. ALCANCE

Inicia con la solicitud en el software de mesa de ayuda, la recibe el profesional especializado 1 - Ingeniero de calidad y seguridad, quién lleva la traza de las solicitudes autorizadas y reasigna la solicitud al responsable de asignar los usuarios, roles y privilegios en cada sistema de información o herramienta tecnológica y termina con el cierre del servicio

3. DEFINICIONES

3.1. Cuenta de usuario:Corresponde al nombre y contraseña que se le asigna a cada persona para que pueda ingresar a la red de Coljuegos, con ello podrá tener acceso a los archivos, carpetas, servicios de informática y demás servicios que ofrezca la red de Coljuegos.

3.2. Computadores personales o PC:Una computadora personal generalmente es usado por un solo usuario, suele estar equipada para cumplir tareas comunes como es navegar por Internet, realizar trabajos de oficina y acceder a los diferentes sistemas de información con que cuenta una organización.

3.3. Dominio:Es un conjunto de computadores que se encuentran conectados en una red que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.

3.4. Perfiles y privilegios:Es la capacidad de una persona para realizar determinadas operaciones o acceder a determinados archivos, carpetas, objetos, etc., los cuales se encuentran residentes en los diferentes equipos que conforman la red de COLJUEGOS.

3.5. Software de oficina:Corresponde a aquellas herramientas que pueden ser utilizadas por la mayoría de los funcionarios de Coljuegos, tales como: Office, spark, Internet, correo electrónico, antivirus y herramientas que trae el sistema operativo Windows para el manejo del PC.

3.6. Redes de Computadores:Es un conjunto de equipos Informáticos y software conectados entre sí por medio de dispositivos físicos, que se usa con la finalidad de compartir información, recursos y ofrecer servicios.

3.7. Roles:Un rol determina lo que puede y lo que no puede hacer un usuario dentro de un

Figura 2. (Continuación)

instructivo

<http://aplicacionpro/ISOpcion/bancoconocimiento/GGESTIONDEC...>

sistema. Los administradores funcionales de cada sistema usan los roles para agrupar los privilegios en conjuntos que pueden asignarse a cuentas de usuario. Los usuarios asociados con un rol tienen todos los privilegios que incluye el rol. Cuando a una cuenta de usuario se le asignan varios roles, el usuario recibe todos los privilegios de cada uno de esos roles.

4. POLITICAS

[POLÍTICAS MACRO PROCESO GESTIÓN DE TIC](#)

5. ACTIVIDADES

1. Los titulares de las Oficinas, Vicepresidencias y Gerentes de Coljuegos, solicitan a través de la herramienta de mesa de ayuda y por el proyecto de "Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos", para su personal a cargo, la creación cuentas de usuarios y asignación de roles y privilegios para los sistemas correspondientes. El titular, en el campo descripción de la solicitud, describirá los Roles, Perfiles y Permisos de cada aplicación. Para mayor detalle ver documento de Roles, Perfiles y Permisos de cada aplicación.
2. Dependiendo del tipo de solicitud, el profesional especializado 1 (Ingeniero de Seguridad y Calidad) reasigna el servicio al líder funcional de cada sistema. Así mismo, monitorea la solicitud para que sea atendida y llevará la traza de las solicitudes autorizadas.
3. Si la solicitud es creación cuenta de red, spark o correo electrónico, el Profesional 1 (Administrador de redes y comunicaciones) realiza las siguientes actividades:
 - Crea en el servidor de dominio la cuenta de usuario con los perfiles y privilegios autorizados por los titulares de las oficinas asesoras y Vicepresidencias, de acuerdo a la información diligenciada en el servicio. El nombre de la cuenta será el primer carácter del primer nombre y el primer apellido, en caso que coincidan dos o más cuentas, el Profesional 1 (Administrador de redes y comunicaciones), en lugar del primer carácter del nombre colocará los caracteres subsiguientes que permitan que el nombre de la cuenta sea diferente.
 - Reasigna el servicio al técnico 2-Soporte a Usuarios para que se cree el spark y solicite al proveedor el correo electrónico correspondiente, con el mismo nombre de la cuenta de red.
 - El Técnico 2-Soporte a Usuarios, crea las carpetas compartidas para backup de este usuario.
 - El Técnico 2-Soporte a Usuarios, crea la extensión telefónica para este usuario en caso de ser solicitada.
 - El técnico 2-Soporte a Usuarios, gestiona ante el proveedor de servicio la creación de la cuenta de correo electrónico.
 - El técnico 2-Soporte a Usuarios, si no hay más requerimientos en la solicitud, coloca la solicitud en estado resuelto.
 - El sistema c-Innova crea automáticamente la cuenta del usuario con el mismo nombre de la cuenta de red en el software de mesa de ayuda, cuando el usuario ingresa por primera vez.

Nota: El usuario del correo electrónico institucional debe revisar y administrar con frecuencia su buzón, para que el espacio físico asignado no se agote y evite se presente problemas de envío y recepción de mensajes. Para ello será necesario que el usuario elimine los mensajes que no necesita y mantenga sólo los requeridos para su trabajo.

2 de 6

28/06/2016 2:54 p. m.

Figura 2. (Continuación)

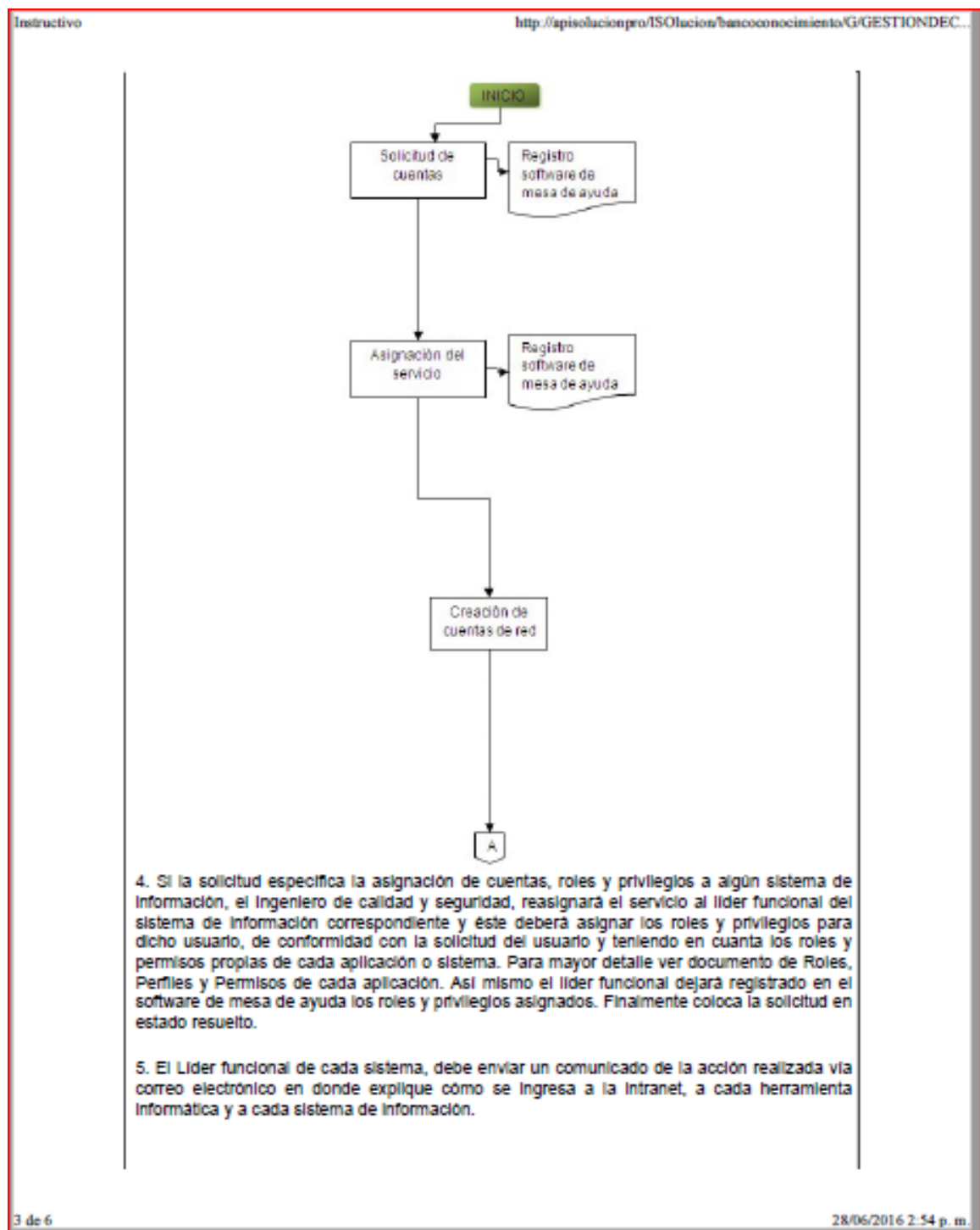


Figura 2. (Continuación)

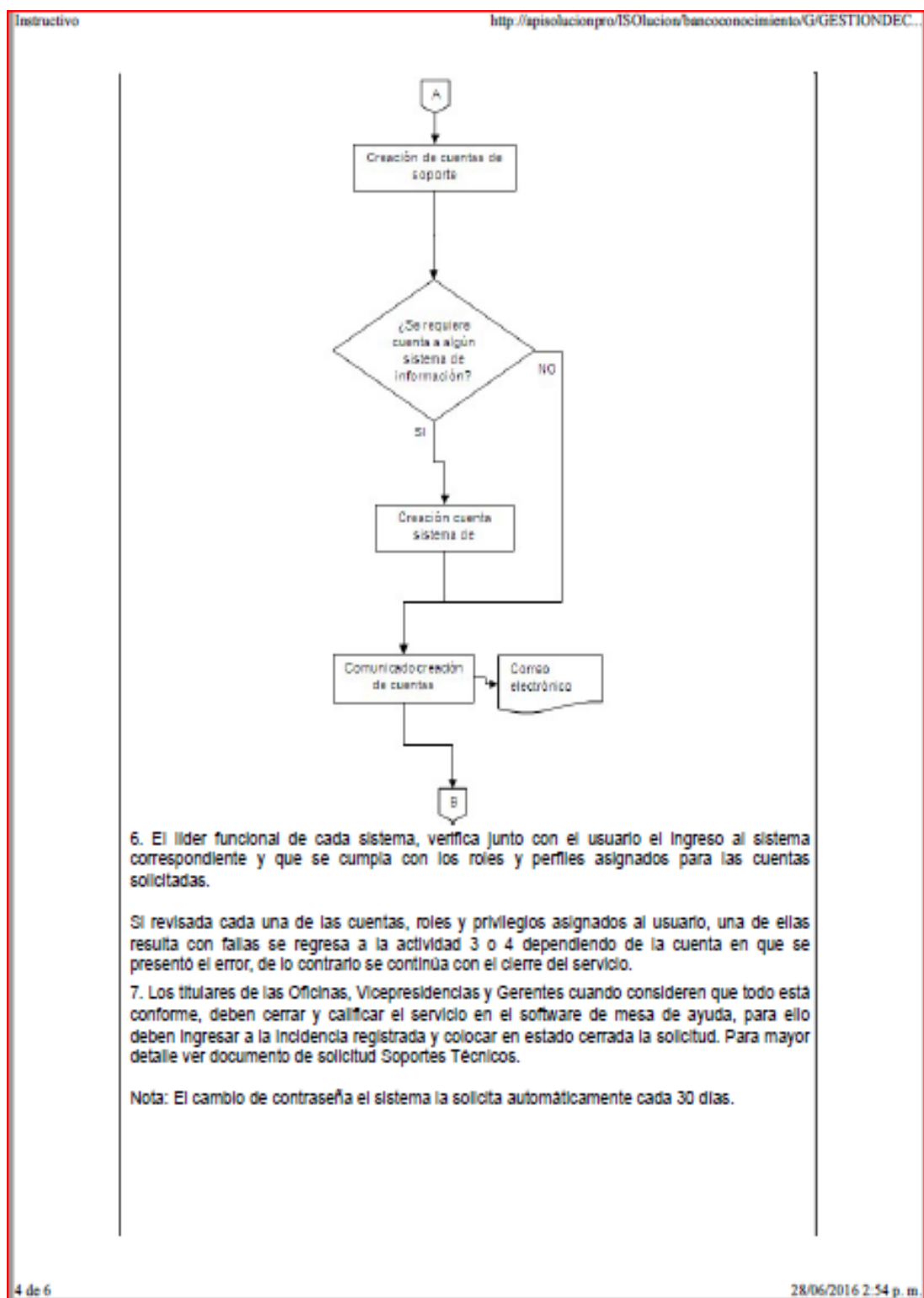


Figura 2. (Continuación)

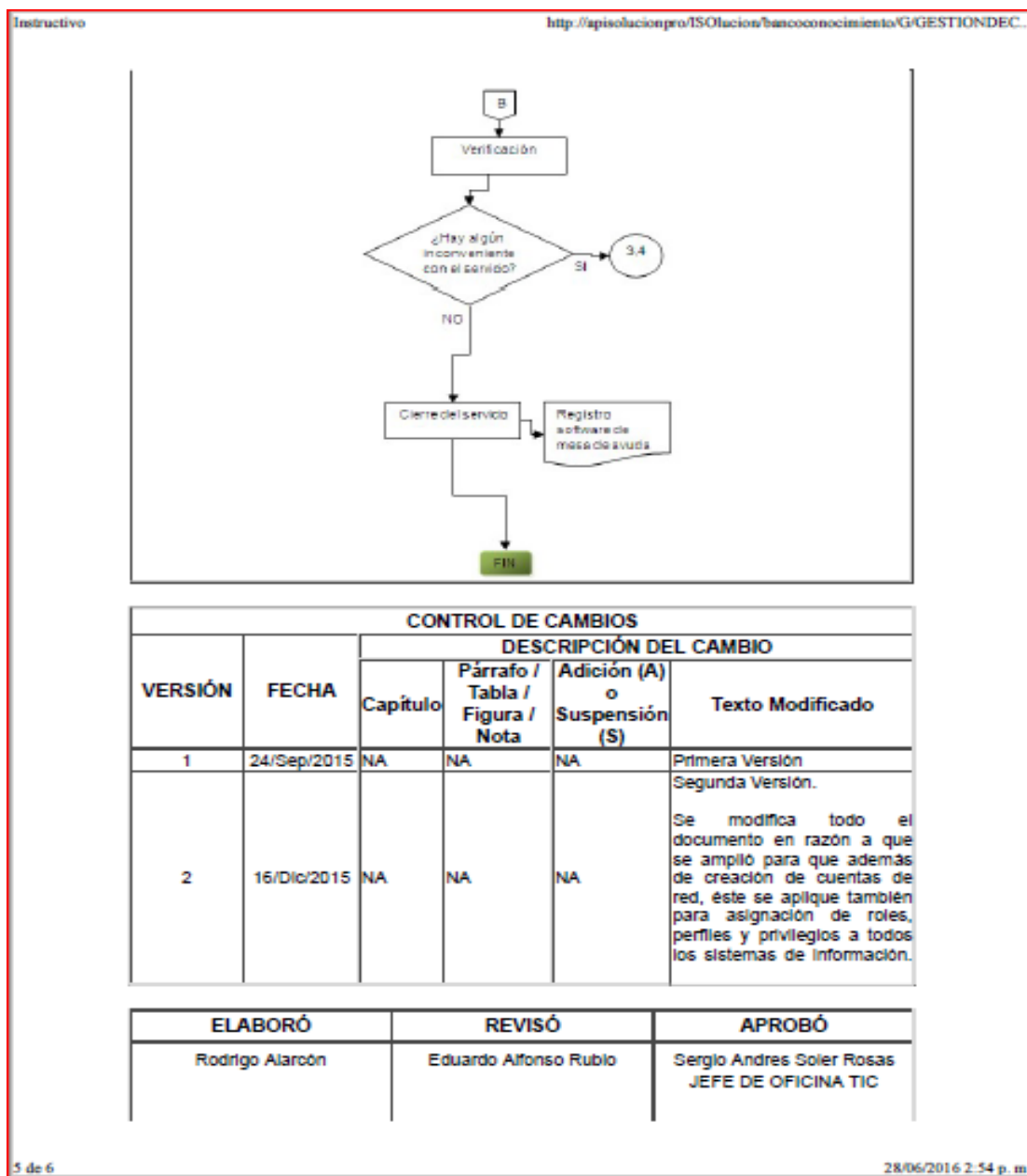
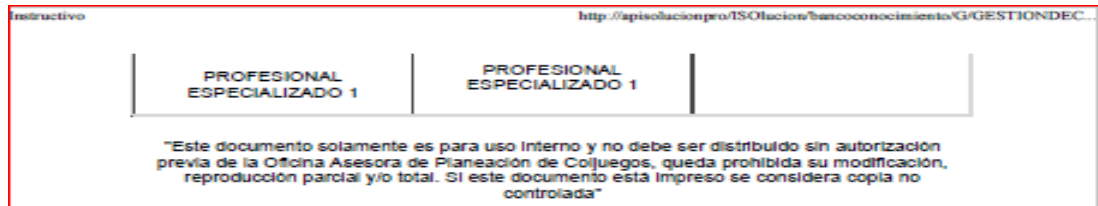


Figura 2. (Continuación)

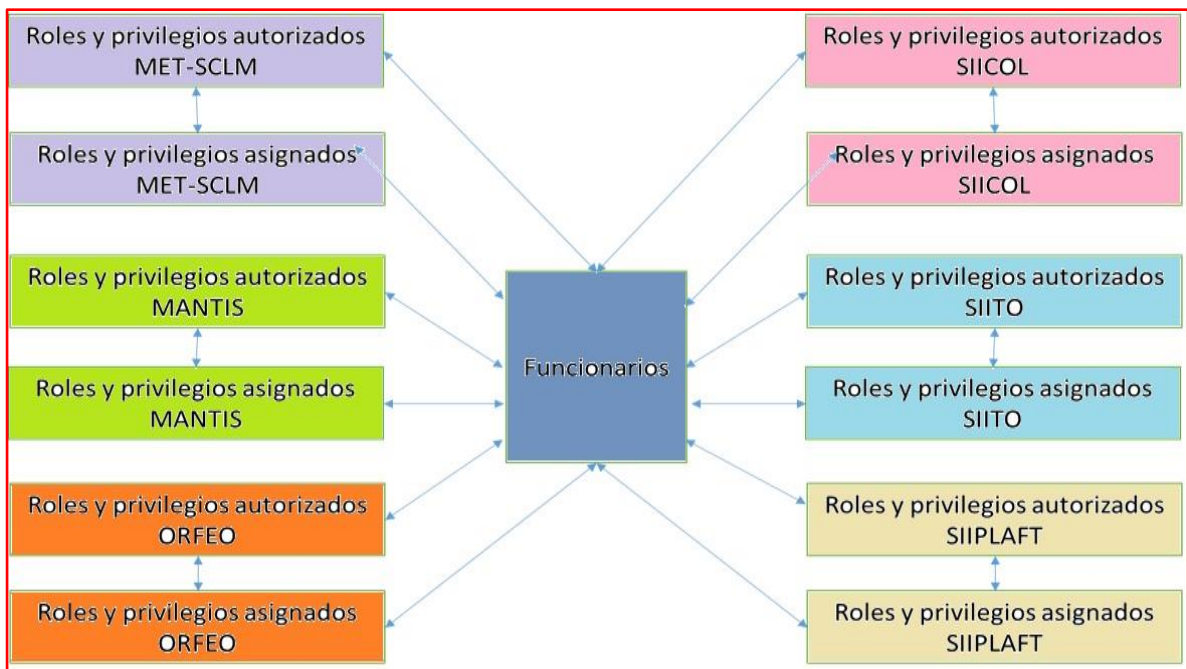


Fuente: autores

5.4 INFORMACIÓN CONSIDERADA EN EL MODELO PARA EL SEGUIMIENTO Y CONTROL DE LA ADMINISTRACIÓN DE USUARIOS, ROLES Y PRIVILEGIOS

La figura 3 muestra la estructura de la información y sus interrelaciones. Contiene información de los usuarios, roles y privilegios **autorizados**, y roles y privilegios **asignados**, por cada de las aplicaciones.

Figura 3. Estructura de la información y sus interrelaciones para el seguimiento y control de la administración de usuarios, roles y privilegios.



Fuente: autores

El modelo está compuesto de las siguientes entidades de información, las cuales se implementaron en Mantis, Access y Excel, así:

- **Funcionarios.** Compuesta de aquellos atributos que permiten identificar a cada funcionario de Coljuegos. Implementada en Access.
- **Roles y Privilegios autorizados de ORFEO.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios autorizados a cada funcionario en el sistema Orfeo, para lo cual se diligencia el formato correspondiente y se adjunta a la solicitud enviada a través del software de mesa de ayuda. Implementada en Mantis y Excel.
- **Roles y Privilegios asignados de ORFEO.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios asignados a cada funcionario en el sistema Orfeo. Esta información se encuentra dentro de las tablas del sistema ORFEO.
- **Roles y Privilegios autorizados de SIICOL.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios autorizados a cada funcionario en el sistema SIICOL, para lo cual se diligencia el formato correspondiente y se adjunta a la solicitud enviada a través del software de mesa de ayuda. Implementada en Mantis y Excel.
- **Roles y Privilegios asignados de SIICOL.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios asignados a cada funcionario en el sistema SIICOL. Esta información se encuentra dentro de las tablas del sistema SIICOL.
- **Roles y Privilegios autorizados de SIPLAFT.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios autorizados a cada funcionario en el sistema SIPLAFT, para lo cual se diligencia el formato correspondiente y se adjunta a la solicitud enviada a través del software de mesa de ayuda. Implementada en Mantis y Excel.
- **Roles y Privilegios asignados de SIPLAFT.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios asignados a cada funcionario en el sistema SIPLAFT. Esta información se encuentra dentro de las tablas del sistema SIPLAFT.
- **Roles y Privilegios autorizados de SCLM-MET** Compuesta de aquellos atributos que permiten identificar los roles y privilegios autorizados a cada funcionario en el sistema SCLM-MET, para lo cual se diligencia el formato correspondiente y se adjunta a la solicitud enviada a través del software de mesa de ayuda. Implementada en Mantis y Excel.
- **Roles y Privilegios asignados de SCLM-MET** Compuesta de aquellos atributos que permiten identificar los roles y privilegios asignados a cada funcionario en el

sistema SCLM-MET. Esta información se encuentra dentro de las tablas del sistema SCLM_MET.

- **Roles y Privilegios autorizados de SIITO.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios autorizados a cada funcionario en el sistema SIITO, para lo cual se diligencia el formato correspondiente y se adjunta a la solicitud enviada a través del software de mesa de ayuda. Implementada en Mantis y Excel.
- **Roles y Privilegios asignados de SIITO.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios asignados a cada funcionario en el sistema SIITO. Esta información se encuentra dentro de las tablas del sistema SIITO.
- **Roles y Privilegios autorizados de MANTIS.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios autorizados a cada funcionario en el sistema MANTIS, para lo cual se diligencia el formato correspondiente y se adjunta a la solicitud enviada a través del software de mesa de ayuda. Implementada en Mantis y Excel.
- **Roles y Privilegios asignados de MANTIS.** Compuesta de aquellos atributos que permiten identificar los roles y privilegios asignados a cada funcionario en el sistema MANTIS. Esta información se encuentra dentro de las tablas del sistema MANTIS.

5.4.1 Estructura de información de los funcionarios. Esta estructura registrará información básica de todos los funcionarios de Coljuegos, porque a cualquiera de ellos con las debidas autorizaciones se les puede asignar roles y privilegios en cada una de los sistemas de información. Se deben tener también en cuenta los funcionarios encargados de asignar los diferentes roles y privilegios en cada uno de los sistemas de información, porque a ellos se le deben asignar las solicitudes recibidas a través de mantis.

El cuadro 2, describe cada uno de los atributos de la estructura funcionarios:

Cuadro 2. Atributos de la estructura funcionarios:

Estructura Funcionarios	
Nombre Atributo	Descripción Atributo
Cuenta	Cuenta creada para cada funcionario en el Directorio Activo de Windows
Cédula	Número de cédula del funcionario
Nombre	Nombre y apellidos del funcionario
Tipo vinculación	Indica si es Empleado Público, Trabajador Oficial, trabajador en misión, Trabajador por Honorarios
Cargo	Grado del Cargo a ocupar dentro de la planta de personal
Denomina cargo	Denominación del cargo
Fe ingreso	Fecha de ingreso del funcionario
fec nacimiento	Fecha de nacimiento del funcionario
dependencia	Dependencia o área donde labora
mantis-ing-ret	Número del mantis que generó la incidencia de ingreso o retiro
fec mantis	Fecha del mantis que generó el ingreso o retiro
activo	Estado del funcionario Activo= SI o No activo=NO
orfeo	El funcionario se encuentra con acceso a ORFEO = SI o NO
Mantis-Auto Orfeo	Número del mantis que autorizó el acceso al sistema ORFEO
siplaft	El funcionario se encuentra con acceso a SIPLAFT = SI o NO
Mantis-AutoSiplaft	Número del mantis que autorizó el acceso al sistema SIPLAFT
met	El funcionario se encuentra con acceso a SCLM-MET = SI o NO
Mantis-AutoMet	Número del mantis que autorizó el acceso al sistema SCLM_MET
siito	El funcionario se encuentra con acceso a SIITO = SI o NO
Mantis-AutoSiito	Número del mantis que autorizó el acceso al sistema SIITO
siicol	El funcionario se encuentra con acceso a SIICOL = SI o NO
Mantis-AutoSiicol	Número del mantis que autorizó el acceso al sistema SIICOL
baloto	El funcionario se encuentra con acceso a BALOTO = SI o NO
mantis-autoBaloto	Número del mantis que autorizó el acceso al sistema BALOTO
carpetascompartidas	El funcionario se encuentra con acceso a carpetas compartidas = SI o NO
mantis-autocarpetas	Número del mantis que autorizó el acceso a carpetas compartidas
sara	El funcionario se encuentra con acceso a SARA = SI o NO
Mantis-Auto Sara	Número del mantis que autorizó el acceso al sistema SARA
sireci	El funcionario se encuentra con acceso a SIRECI = SI o NO
Mantis-sireci	Número del mantis que autorizó el acceso al sistema SIRECI
isolucion	El funcionario se encuentra con acceso a ISOLUCION = SI o NO
Mantis-isolucion	Número del mantis que autorizó el acceso al sistema ISOLUCION

Fuente: autores

5.4.2 Estructura de información de las novedades de personal. Información que debe suministrar la gerencia de Talento Humano a la Oficina de TI, sobre las novedades de personal a través del software de mesa de ayuda, Cuadro 3, así por ejemplo para los ingresos de personal nuevo, suministra los siguientes datos, los cuales el ingeniero de Seguridad y Calidad registra en la estructura de funcionarios:

Cuadro 3. Estructura de funcionarios

Nombre Atributo	Descripción Atributo
cédula	Número de cédula del funcionario
nombre	Nombre del funcionario
Tipo vinculación	Indica si es empleado Público, Trabajador Oficial, trabajador en misión, Trabajador por Honorarios
cargo	Grado del Cargo a ocupar dentro de la planta de personal
denomina cargo	Denominación del cargo
fe ingreso	Fecha de ingreso del funcionario
fec nacimiento	Fecha de nacimiento del funcionario
dependencia	Dependencia o área donde labora

Fuente: autores

Otras novedades que la Gerencia de Talento Humano debe suministrar a través del software de mesa de ayuda con los datos correspondientes, son las siguientes:

- Cambio vinculación laboral
- Incapacidades por enfermedad o por accidente
- Ingresos de Personal
- Licencias de maternidad o paternidad
- Licencias No remuneradas
- Permisos de personal
- Retiro de personal
- Traslados internos de personal
- Vacaciones de Personal


5.4.3 Formatos para solicitar roles y permisos por cada una de las aplicaciones de Coljuegos.

Otra importante información son los roles y privilegios autorizados a cada funcionario en cada una de los sistemas de información a través de software de mesa de ayuda. Esta información la suministra por los Jefes de Oficina, Vicepresidentes y Gerentes.

Para facilitar esta labor se diseñó por cada aplicación un formato que contiene los roles y privilegios a ser autorizados, los cuales se muestran a continuación en las figuras 4, 5, 6, 7 y 8.


Formato para el ingreso de roles y perfiles MANTIS

Figura 4. Registro de roles y perfiles

	REGISTRO DE ROLES Y PERFILES (Lider Funcional MANTIS)		Versión 001							
			Código REG - IT - 001							
			Página 1 de 1							
			Fecha 20 / 02 / 2016							
		Fecha:		<table border="1"><tr><td>Día</td><td>Mes</td><td>Año</td></tr><tr><td></td><td></td><td></td></tr></table>	Día	Mes	Año			
Día	Mes	Año								
1. Información del Usuario										
Apellidos:		Nombres:								
Cargo:		Área:								
Fecha de finalización del contrato										
2. Roles (Sistema de información Mantis)										
<input type="checkbox"/> Administrador <input type="checkbox"/> Manager <input type="checkbox"/> Desarrollador <input type="checkbox"/> Actualizador <input type="checkbox"/> Informador <input type="checkbox"/> Espectador										
2. Permisos (Sistema de información Mantis)										
<input type="checkbox"/> Mi Vista <input type="checkbox"/> Ver Incidencias <input type="checkbox"/> Reportar Incidencia <input type="checkbox"/> Registro de Cambios <input type="checkbox"/> Roadmap <input type="checkbox"/> Resumen <input type="checkbox"/> Administración <input type="checkbox"/> Mi Cuenta										
3. Observaciones										
4. Firma de Director del Sistema de Información										
<div style="border-top: 1px solid black; text-align: center; margin-top: 20px;">Firma</div>										


Fuente: autores

Figura 5. Formato para el ingreso de roles y perfiles SIPLAFT

	REGISTRO DE ROLES Y PERFILES (Lider Funcional SIPLAFT)		Versión 001							
			Código REG - IT - 001							
			Página 1 de 1							
			Fecha 20 / 02 / 2016							
Fecha: <table border="1"> <tr> <td>Día</td> <td>Mes</td> <td>Año</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>					Día	Mes	Año			
Día	Mes	Año								
1. Información del Usuario										
Apellidos:				Nombres:						
Cargo:				Area:						
Fecha de finalización del contrato										
2. Roles (Sistema de Información Siplaft)										
<input type="checkbox"/> Administradores <input type="checkbox"/> Operadores										
2. Permisos (Sistema de Información Siplaft)										
Administración de Usuarios	<input type="checkbox"/> Ingresar	<input type="checkbox"/> Consultar	<input type="checkbox"/> Modificar	<input type="checkbox"/> Borrar						
Cargue Formularios	<input type="checkbox"/> Ingresar	<input type="checkbox"/> Consultar	<input type="checkbox"/> Modificar	<input type="checkbox"/> Borrar						
Consulta Acuses de Recibo	<input type="checkbox"/> Ingresar	<input type="checkbox"/> Consultar	<input type="checkbox"/> Modificar	<input type="checkbox"/> Borrar						
3. Observaciones										
4. Firma de Director del Sistema de Información										
<div style="text-align: center;"> _____ Firma </div>										


Fuente: autores

Figura 6. Formato para el ingreso de roles y perfiles SIITO

	REGISTRO DE ROLES Y PERFILES (Lider Funcional SIITO)		Versión 001								
			Código REG - IT - 001								
			Página 1 de 1								
			Fecha 20 / 02 / 2016								
					Fecha: <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Día</td> <td style="width: 20px; text-align: center;">Mes</td> <td style="width: 20px; text-align: center;">Año</td> </tr> <tr> <td style="height: 20px;"></td> <td></td> <td></td> </tr> </table>	Día	Mes	Año			
Día	Mes	Año									
1. Información del Usuario											
Apellidos:				Nombres:							
Cargo:				Área:							
Fecha de finalización del contrato											
2. Roles (Sistema de Información SIITO)											
<input type="checkbox"/> Administrador <input type="checkbox"/> Operador <input type="checkbox"/> Coordinador SAC <input type="checkbox"/> Coordinador DME <input type="checkbox"/> Coordinador GAP <input type="checkbox"/> Analista SAC <input type="checkbox"/> Analista DME <input type="checkbox"/> Analista GAP <input type="checkbox"/> Analista Calidad DME											
2. Permisos (Sistema de Información SIITO)											
<input type="checkbox"/> Administración usuarios <input type="checkbox"/> Diligenciamiento y Cargue formularios <input type="checkbox"/> Asignar Analista <input type="checkbox"/> Verificar, validar, aprobar, rechazar, Solicitud <input type="checkbox"/> Desiste solicitud <input type="checkbox"/> Generar requerimiento <input type="checkbox"/> Responder requerimiento											
3. Observaciones											
4. Firma de Director del Sistema de Información											
<div style="border-top: 1px solid black; width: 100%; margin-bottom: 5px;"></div> Firma											


Fuente: autores

Figura 7. Formato para el ingreso de roles y perfiles ORFEO

		REGISTRO DE ROLES Y PERFILES (Lider Funcional ORFEO)		Versión: 001							
				Código REG - IT - 001							
				Página 1 de 1							
				Fecha: 20 / 02 / 2016							
				Fecha: <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Dia</td> <td style="width: 20px; text-align: center;">Mes</td> <td style="width: 20px; text-align: center;">Año</td> </tr> <tr> <td style="height: 20px;"></td> <td></td> <td></td> </tr> </table>		Dia	Mes	Año			
Dia	Mes	Año									
1. Información del Usuario											
Apellidos:				Nombres:							
Cargo:				Área:							
Fecha de finalización del contrato											
2. Roles (Sistema de Información Orfeo)											
<input type="checkbox"/> Administrador <input type="checkbox"/> Canal de Distribución <input type="checkbox"/> Canal PQRD <input type="checkbox"/> Usuario Normal											
2. Permisos (Sistema de Información Orfeo)											
<input type="checkbox"/> Digitalización de Documentos (0-2)	<input type="text"/>	<input type="checkbox"/> Préstamo de Documentos		<input type="checkbox"/> (9) Históricas (0-3)	<input type="text"/>						
<input type="checkbox"/> Modificaciones		<input type="checkbox"/> Anulaciones		<input type="checkbox"/> Reporte Radicación							
<input type="checkbox"/> Impresión (0-2)	<input type="text"/>	<input type="checkbox"/> Devoluciones de Correo		<input type="checkbox"/> (2) Entrada (0-1)	<input type="text"/>						
<input type="checkbox"/> Solicitud de Anulaciones		<input type="checkbox"/> Envío de Correo		<input type="checkbox"/> (8) PQRD (0-3)	<input type="text"/>						
<input type="checkbox"/> Administrador de Archivo (0-2)	<input type="text"/>	<input type="checkbox"/> Estadísticas (0-2)	<input type="text"/>	<input type="checkbox"/> Puede borrar Anexos .Jif							
<input type="checkbox"/> Administrador del Sistema		<input type="checkbox"/> Nivel de Seguridad (1-5)	<input type="text"/>	<input type="checkbox"/> Se autentica por medio de LDAP							
<input type="checkbox"/> Usuario Reasigna		<input type="checkbox"/> Firma Digital (0-2)	<input type="text"/>	<input type="checkbox"/> Puede Asignar Premiado							
<input type="checkbox"/> Usuario Nuevo		<input type="checkbox"/> Usuario Público		<input type="checkbox"/> Puede Tipificar Anexos .Jif							
<input type="checkbox"/> Puede Archivar Documentos		<input type="checkbox"/> Notificación de Resoluciones		<input type="checkbox"/> Puede utilizar el editor de Flujos							
<input type="checkbox"/> Creación de expedientes (0-2)	<input type="text"/>	<input type="checkbox"/> Trámite Respuesta Radicado		<input type="checkbox"/> Resolución (0-3)	<input type="text"/>						
<input type="checkbox"/> Remitenes / Terceros		<input type="checkbox"/> Radicación Express (0-3)	<input type="text"/>	<input type="checkbox"/> Autos (0-3)	<input type="text"/>						
<input type="checkbox"/> Tablas de Retención Documental		<input type="checkbox"/> (1) Salida		<input type="checkbox"/> Circulares (0-3)	<input type="text"/>						
<input type="checkbox"/> Radicación Masiva		<input type="checkbox"/> (2) Interna (0-3)	<input type="text"/>								
3. Observaciones											
4. Firma de Director del Sistema de Información											
_____ Firma											

Fuente: autores

Figura 8. Formato para el ingreso de roles y perfiles MET-SCLM

	REGISTRO DE ROLES Y PERFILES (Lider Funcional MET-SCLM)		Versión 001								
			Código REG - IT - 001								
			Página 1 de 1								
			Fecha 20 / 02 / 2016								
					Fecha: <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Dia</td> <td style="width: 20px; text-align: center;">Mes</td> <td style="width: 20px; text-align: center;">Año</td> </tr> <tr> <td style="height: 20px;"></td> <td style="height: 20px;"></td> <td style="height: 20px;"></td> </tr> </table>	Dia	Mes	Año			
Dia	Mes	Año									
1. Información del Usuario											
Apellidos:				Nombres:							
Cargo:		Área:									
Fecha de finalización del contrato											
2. Roles (Sistema de Información Met-SCLM)											
<input type="checkbox"/> Administrador <input type="checkbox"/> Operador <input type="checkbox"/> Coordinador SAC <input type="checkbox"/> Coordinador DME <input type="checkbox"/> Coordinador GAP											
<input type="checkbox"/> Analista SAC <input type="checkbox"/> Analista DME <input type="checkbox"/> Analista GAP <input type="checkbox"/> Analista Calidad DME											
2. Permisos (Sistema de Información Met-SCLM)											
<input type="checkbox"/> Administración usuarios		<input type="checkbox"/> Diligenciamiento y Cargue formularios		<input type="checkbox"/> Asignar Analista							
<input type="checkbox"/> Desiste solicitud		<input type="checkbox"/> Generar requerimiento		<input type="checkbox"/> Verificar, validar, aprobar, rechazar, Solicitud							
				<input type="checkbox"/> Responder requerimiento							
3. Observaciones											
4. Firma de Director del Sistema de Información											
_____ Firma											

Fuente: autores

Con toda la anterior información, se logra el seguimiento y control de la administración de usuarios, roles y privilegios asignados a los sistemas de información de Coljuegos, básicamente por tres grandes componentes: Primero la información de los funcionarios; segundo los roles y privilegios que se **asignan** a cada funcionario en cada uno de los sistemas de información y tercero los roles y privilegios **autorizados** a través del software de mesa de ayuda por los Jefes de Oficina, Vicepresidentes y Gerentes a cada funcionario en cada uno de los sistemas de información.

Los roles y perfiles **asignados** se encuentran en las tablas correspondientes a cada sistema de información y los asigna el líder de cada sistema, a través del módulo implementado para ello.

Para los roles y perfiles **autorizados**, se crearon los respectivos formatos que facilitan a los Jefes de Oficina, Vicepresidentes y Gerentes, que sus solicitudes vengan bien detalladas, especificando que rol y privilegio, se desea sea asignado a cada funcionario en cada uno de los sistemas de información. Una vez se tenga la solicitud bien diligenciada, el paso siguiente es registrar esta información en las tablas de autorizaciones para cada sistema de información.

5.5 HERRAMIENTAS INFORMÁTICAS CONSIDERADAS PARA EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS

Se adicionó un nuevo proyecto en el software de mesa de ayuda - MANTIS, denominado “Gestión de usuarios, cuentas, roles y privilegios”. En este proyecto se adicionaron las categorías correspondientes. Dichas categorías están compuestas de cada sistema de información y las novedades que puede haber sobre el personal de Coljuegos. De esta manera se puede llevar un mejor control y seguimiento de los accesos. La traza de estas solicitudes quedará en la mesa de ayuda. El control y seguimiento se realizará con base a estos elementos y a los datos de entrada, los cuales ya fueron considerados en el anterior numeral 5.4.

A continuación, se muestran las categorías creadas en el software Mantis para el proyecto Gestión cuentas de usuarios, Roles, perfiles y Permisos, las cuales corresponden a accesos a recursos específicos, asignación de cuentas, roles y privilegios por cada uno de los sistemas de información y las novedades de personal.

Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos

- Acceso a Carpetas Compartidas
- Acceso a VPN

- Acceso Escritorio remoto de Servidores
- Acceso Escritorio Remoto de Usuarios
- Asignación Cuentas, Roles y Privilegios BD SQL SERVER
- Asignación Cuentas, Roles y Privilegios DIGITURNO
- Asignación Cuentas, Roles y Privilegios INTRANET – CINNOVA
- Asignación Cuentas, Roles y Privilegios SARA
- Asignación Cuentas, Roles y Privilegios BALOTO
- Asignación Cuentas, Roles y Privilegios BD ORACLE
- Asignación Cuentas, Roles y Privilegios CHARRY
- Asignación Cuentas, Roles y Privilegios CONTROL ACCESO BIOMÉTRICO
- Asignación Cuentas, Roles y Privilegios CORREO ELECTRÓNICO
- Asignación Cuentas, Roles y Privilegios ELASTIX
- Asignación Cuentas, Roles y Privilegios ISO LUCIÓN
- Asignación Cuentas, Roles y Privilegios MANTIS
- Asignación Cuentas, Roles y Privilegios MET
- Asignación Cuentas, Roles y Privilegios ORFEO
- Asignación Cuentas, Roles y Privilegios PORTAL WEB
- Asignación Cuentas, Roles y Privilegios RED COLJUEGOS
- Asignación Cuentas, Roles y Privilegios SIICOL
- Asignación Cuentas, Roles y Privilegios SIITO
- Asignación Cuentas, Roles y Privilegios SIVICAL
- Asignación Cuentas, Roles y Privilegios SPARK

- Asignación Cuentas, Roles y Privilegios SVN TORTOISE
- Cambio vinculación laboral
- Incapacidades por enfermedad o por accidente
- Ingresos de Personal
- Licencias de maternidad o paternidad
- Licencias No remuneradas
- Permisos de personal
- Retiro de personal
- Traslados internos de personal
- Vacaciones de Personal

La figura 9 muestra dichas categorías, directamente desde la herramienta mantis:

Figura 9. Categorías creadas en mantis para la administración de usuarios, roles y privilegios.

Conectado como: ralarcon (Rodrigo Alarcón Avila - administrador) 03-05-2016 09:05 COT Proyecto: Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos Cambiar

Principal | Mi Vista | Ver Incidencias | Reportar Incidencia | Registro de cambios | Roadmap | Resumen | Administración | Mi Cuenta | Cerrar Sesión Incidencia # 118

Visitas recientemente: 0012245, 0016314, 0016399, 0017931, 0012912

Introduzca los detalles de la incidencia.

Categoría (seleccionar)

Reproducibilidad (seleccionar)

Severidad

Prioridad

Seleccionar perfil

☐ O complete los siguientes campos

Plataforma

SO

Versión de SO

Asignar a

Resumen

Descripción

Pasos para reproducir

Información Adicional

(seleccionar)

Acceso a Carpetas Compartidas

Acceso a VPN

Acceso Escritorio remoto de Servidores

Acceso Escritorio Remoto de Usuarios

Acceso y Permisos a Internet

Acceso y permisos DVD, USB del equipo

Asignación Cuentas, Roles y Privilegios BD SQL SERVER

Asignación Cuentas, Roles y Privilegios DIGITURNO

Asignación Cuentas, Roles y Privilegios IIS

Asignación Cuentas, Roles y Privilegios INTRANET - CINNOVA

Asignación Cuentas, Roles y Privilegios SARA

Asignación Cuentas, Roles y Privilegios UTM

Asignación Cuentas, Roles y Privilegios ADP- Apuestas Deportivas Paramutuales

Asignación Cuentas, Roles y Privilegios ARCGIS

Asignación Cuentas, Roles y Privilegios ASCENDO - Evaluación Desempeño

Asignación Cuentas, Roles y Privilegios DATASOURCE

Asignación Cuentas, Roles y Privilegios BD ORACLE

Asignación Cuentas, Roles y Privilegios CHARRY

Asignación Cuentas, Roles y Privilegios CONTROL ACCESO BIOMETRICO

Asignación Cuentas, Roles y Privilegios CONTROL ACCESO VISITANTES

Asignación Cuentas, Roles y Privilegios CORREO ELECTRONICO

Asignación Cuentas, Roles y Privilegios DATA PROTECTION MANAGER

Asignación Cuentas, Roles y Privilegios ELASTIX

Asignación Cuentas, Roles y Privilegios FTP-FILE ZILLA

Asignación Cuentas, Roles y Privilegios FURAG-DAFP

Asignación Cuentas, Roles y Privilegios GEOREFERENCIACIÓN - Google Map

Asignación Cuentas, Roles y Privilegios INTERNET

Asignación Cuentas, Roles y Privilegios ISOLUCION

Asignación Cuentas, Roles y Privilegios MANTIS

Asignación Cuentas, Roles y Privilegios MET

Asignación Cuentas, Roles y Privilegios ORFEO

Asignación Cuentas, Roles y Privilegios PORTAL WEB

Asignación Cuentas, Roles y Privilegios PRUEBAS PSICOTÉCNICAS

Asignación Cuentas, Roles y Privilegios RED COLJUEGOS

Asignación Cuentas, Roles y Privilegios SIICOL

Asignación Cuentas, Roles y Privilegios SIIF-MHCP

Asignación Cuentas, Roles y Privilegios SIITO

Asignación Cuentas, Roles y Privilegios SIPLAFT

Asignación Cuentas, Roles y Privilegios SISTEMA DE CAMARAS

Asignación Cuentas, Roles y Privilegios SMGI-MHCP

Asignación Cuentas, Roles y Privilegios SPARK

Asignación Cuentas, Roles y Privilegios SUIT-DAFP

Asignación Cuentas, Roles y Privilegios SUPERASTRO

Asignación Cuentas, Roles y Privilegios SVN TORTOISE

Asignación Cuentas, Roles y Privilegios SYSTEM CENTER

Asignación Cuentas, Roles y Privilegios TOAD

Asignación Cuentas, Roles y Privilegios WEB LOGIC

Asignación Cuentas, Roles y Privilegios RVCC-SUPERSALUD- Recepción, Validación, Cargue y Consulta

Cambio vinculación laboral

Comisiones dentro del país

Comisiones en el exterior

Comisiones transitorias Coljuegos

Encargos

Incapacidades por enfermedad o por accidente

Ingresos de Personal

Licencias de maternidad o paternidad

Licencias No remuneradas

Permisos de personal

Retiro de personal

Traslados internos de personal

Vacaciones de Personal

Fuente: autores

La figura 10 muestra un ejemplo de la información a ser ingresada cuando se envía una solicitud por el proyecto de gestión de usuarios, roles y permisos.

Figura 10. Solicitud para ingreso de personal en la gestión de cuentas de usuarios, roles y privilegios mantis.

ID	Proyecto	Categoría	Visibilidad	Fecha de envío	Última actualización
0013723	Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos	Ingresos de Personal	privado	02-12-2015 18:36	18-12-2015 16:37
Informador	haramendiz				
Asignada a	Otorres				
Prioridad	alta	Severidad	mayor	Reproducibilidad	siempre
Estado	resuelta	Resolución	corregida		
Plataforma		SO		Versión de SO	
Resumen	0013723: Ingresos Planta Coljuegos				
Descripción	<p>Por medio de la presenta incidencia, notifico que el 07 de diciembre ingresan a la planta de Coljuegos las siguientes personas:</p> <ul style="list-style-type: none"> - Miguel José Paz Muñoz c.c. 79.640.134 07/03/1974 Profesional 1 Control Interno - Claudia Patricia Peinado Isaza c.c. 40.612.922 03/09/1984 Profesional 1 Cobro - Juan Camilo Calonje Londoño c.c. 80.854.756 25/09/1985 Profesional 1 Vicepresidencia de Desarrollo Organizacional <p>Lo anterior para los fines pertinentes.</p> <p>Gcs</p> <p>Heidy Araméndiz Pacheco</p>				

Fuente: autores

5.6 CONSULTAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS

Como Coljuegos no tiene los recursos económicos para adquirir un IAM, el Ingeniero de Seguridad y Calidad, se tendrá que ayudar con el software de mesa de ayuda para llevar la traza de las autorizaciones, el software Access para mantener actualizada la información de la tabla de funcionarios y Excel para las tablas de autorizaciones de cada sistema de información, así como también los diferentes reportes para un buen control y seguimiento de usuarios, roles y privilegios.

El sistema implementado, permite realizar las siguientes consultas y reportes, los cuales podrán generarse en una segunda etapa a través de un lenguaje de programación. En esta primera fase y alcance de este proyecto, estas consultas y reportes se realizan utilizando las herramientas Mantis, Access y Excel.

- ¿Qué funcionarios se encuentran activos en cada uno de los sistemas de información?

Lo anterior se logra extractando de la base de datos de cada sistema de información, los usuarios, roles y permisos asignados. En el cuadro 4 siguiente, se presenta una muestra de algunos usuarios (cuentas) y roles asignados para el sistema SIICOL.

Cuadro 4. Muestra de algunos usuarios

Usuario	Rol asignado
AALDANA	Coordinador COI
AALFONSO	Auxiliar DME GNN
AALFONSO	Área Solicitante CAD I
AÁLVAREZ	Área Usuario Tesorería
AÁLVAREZ	Área Usuario Cartera
AÁLVAREZ	Técnico II Tesorería
ABLANCO	Funcionarios VO
ABLANCO	Auxiliar Cartera GCT
ABLANCO	Profesional-Gestor de información
ABLANCO	Usuario Reporte Inventario GCT
ABLANCO	Reporte Directorio Localizados
ACASTELBLANCO	Auxiliar Gestión Contable III
ACASTILLO	Área Usuario Gestión Contable
ACASTILLO	Administrador Sesiones
ACASTILLO	Área Usuario Tesorería
ACASTILLO	Área Usuario Cartera
ACASTILLO	Área Usuario Contratación Administrativa
ACASTILLO	Auxiliar Tesorería
ACASTILLO	Usuario Reporte Inventario GCT
ACASTILLO	Área Usuario Presidencia
ACLAVIJO	Funcionario 3 GPCOI
ACLAVIJO	Funcionario 4 GPCOI
ACLAVIJO	Auxiliar Cartera GCT
ACLAVIJO	Usuario Reporte Inventario GCT
ACLAVIJO	Gestor de información COI
ACLAVIJO	Funcionario 2 GPCOI
A CLAVIJO	Funcionario 1 GPCOI
A HERNÁNDEZ	Aprobador póliza localizados
A LÓPEZ	Área Solicitante CAD I
AMORALES	Auxiliar CAD I

Continuación Cuadro 4. Muestra de algunos usuarios

Usuario	Rol asignado
A PARCILA	Usuario Reporte Inventario GCT
A PARCILA	CN Analista GNA
APARCILA	Auxiliar Cartera GCT
AP RAMÍREZ	Área Solicitante CAD I
AURREGO	Área Usuario GCT
AURREGO	Profesional - Gestor de Control
AVANEGAS	Profesional - Gestor de Control
BABRIL	Auxiliar CAD I
CA HERNÁNDEZ	Grupo sustanciadores - Fiscalización
CA HERNÁNDEZ	Funcionarios VO
CAHUMADA	PR Analista GNA
CAHUMADA	PR Notificaciones SAC
CCARDOZO	Área Solicitante CAD I
CFIERRO	Jefe Área Solicitante CAD
C GÓMEZ	Auxiliar Cartera GCT
C GÓMEZ	Audidores de campo
C GUERRERO	Funcionario 3 GPCOI
CMEDINA	Usuario Reporte Inventario GCT
CMEDINA	Auxiliar Cartera GCT
CMEDINA	CN Analista GNA
CMONTANA	Área Solicitante CAD I

Fuente: autores

Así mismo, la siguiente figura 11, muestra que el rol “Coordinador COI” del sistema SIICOL, tiene acceso a una serie de módulos y las acciones (registrar, modificar, borrar, imprimir, aprobar, rechazar, consultar o devolver) que puede realizar en ellos.

Figura 11. Muestra de algunos roles y permisos de SIICOL

Rol	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Ejecutor Manual Procesos Cartera	S									
Ejecutor Manual Procesos Cartera	S									
Jefe Área Solicitante CAD	S	S	S	S	S	S	S	S	S	S
Jefe Área Solicitante CAD							S			
Jefe Área Solicitante CAD	S	S		S	S		S			S
Jefe Área Solicitante CAD	S	S	S	S	S		S	S		S
Jefe Área Solicitante CAD	S	S	S	S	S		S	S		S
Jefes Consultas							S			
Jefes Consultas							S			
Jefes Consultas							S			
Jefes Consultas							S			
Jefes Consultas							S			
Jefes Consultas							S			
Jefes Consultas							S			

Fuente: autores

- Cuáles funcionarios se han retirado de la empresa y aún siguen activos en los sistemas de información.

Esto se logra cruzando el atributo “activo” (SI o NO) de la estructura funcionarios y la información almacenada de usuarios, roles y permisos en la base de datos de cada sistema de información.

- Cuáles funcionarios están activos en los sistemas de información sin tener autorización para ello.

Esto se logra cruzando la información que se recibe en el software Mantis y la información almacenada de usuarios, roles y permisos en la base de datos de cada sistema de información.

- Cuáles funcionarios tienen más permisos de los autorizados en cada uno de los sistemas de información.

Esto se logra cruzando la información que se recibe en el software Mantis y la información almacenada de usuarios, roles y permisos en la base de datos de cada sistema de información.

- Cuáles funcionarios tienen un rol determinado en un sistema en particular

Esto se logra extractando la información almacenada de usuarios, roles y permisos en la base de datos de cada sistema de información.

- Un funcionario en particular que roles tiene asignado en cada uno de los sistemas.

Esto se logra extractando la información almacenada de usuarios, roles y permisos en la base de datos de cada sistema de información.

- Para el caso de mantis, cuales funcionarios tienen acceso a un proyecto en particular.

Esto se logra extractando la información almacenada de usuarios, roles y permisos en la base de datos del sistema Mantis.

- Para el caso de mantis, un funcionario en particular a qué proyectos tiene acceso y con qué rol.

Esto se logra extractando la información almacenada de usuarios, roles y permisos en la base de datos del sistema Mantis.

- Para el caso de un sistema en particular, por ejemplo, el sistema SIICOL, dado un rol específico, mostrar los módulos y permisos que tiene.

Esto se logra extractando la información almacenada de usuarios, roles y permisos en la base de datos del sistema en particular, para este caso del sistema SIICOL.

- Para el caso de un sistema en particular, por ejemplo, el sistema SIICOL, cuales son los usuarios activos con sus correspondientes roles, módulos y permisos asignados.

Esto se logra extractando la información almacenada de usuarios, roles y permisos en la base de datos del sistema en particular, para este caso del sistema SIICOL.

6. AVANCES OBTENIDOS EN LA APLICACIÓN DEL MODELO

6.1 APLICACIÓN DE LAS NUEVAS POLÍTICAS CORPORATIVAS DE GOBIERNO DE IDENTIDAD, LINEAMIENTOS Y PROCEDIMIENTOS

La aplicación de cada una de las políticas enunciadas en la sección 5.2, así como también los lineamientos y procedimientos explicados en la sección 5.3, de este documento, se ven reflejadas en las siguientes secciones.

La tabla 1 muestra un resumen del número de solicitudes enviadas a través de la herramienta mantis, por los Jefes de oficina, Vicepresidentes y Gerentes, y que fueron atendidas por el proyecto de “gestión de usuarios, roles y permisos”, durante el año 2016 (Figura 13), lo cual se utiliza para el seguimiento y control.

La figura 12 presenta una muestra de las solicitudes colocadas por la Gerencia de Capital Humano, a través de la herramienta mantis durante el año 2016, por la categoría “Ingresos de personal”, lo cual se utiliza para el control y seguimiento.

Tabla 1. Número de solicitudes atendidas en el año 2016 sobre gestión de usuarios, roles y privilegios.

Categorías del proyecto Gestión usuarios, roles y permisos	Número de solicitudes a junio 2016	Número de solicitudes a noviembre 2016
Acceso a Carpetas Compartidas	23	129
Acceso a VPN	1	27
Acceso Escritorio remoto de Servidores	2	2
Acceso Escritorio Remoto de Usuarios	2	4
Acceso y Permisos a Internet	8	36
Acceso y permisos DVD, USB del equipo	1	21
Asignación Cuentas, Roles y Privilegios BD SQL SERVER	1	5
Asignación Cuentas, Roles y Privilegios DIGITURNO	0	3
Asignación Cuentas, Roles y Privilegios INTRANET – CINNOVA	3	6
Asignación Cuentas, Roles y Privilegios SARA	4	14
Asignación Cuentas, Roles y Privilegios UTM	0	1
Asignación Cuentas, Roles y Privilegios BALOTO	0	3
Asignación Cuentas, Roles y Privilegios BD ORACLE	0	2
Asignación Cuentas, Roles y Privilegios CHARRY	0	10
Asignación Cuentas, Roles y Privilegios ACCESO BIOMÉTRICO	4	29
Asignación Cuentas, Roles y Privilegios ACCESO VISITANTES	0	1
Asignación Cuentas, Roles y Privilegios CORREO ELECTRÓNICO	7	44
Asignación Cuentas, Roles y Privilegios ELASTIX	1	2
Asignación Cuentas, Roles y Privilegios INTERNET	6	11
Asignación Cuentas, Roles y Privilegios ISOLUCIÓN	4	44
Asignación Cuentas, Roles y Privilegios MANTIS	4	15
Asignación Cuentas, Roles y Privilegios MET	1	2
Asignación Cuentas, Roles y Privilegios ORFEO	42	181
Asignación Cuentas, Roles y Privilegios PORTAL WEB	2	9
Asignación Cuentas, Roles y Privilegios RED COLJUEGOS	4	48
Asignación Cuentas, Roles y Privilegios SIICOL	29	160
Asignación Cuentas, Roles y Privilegios SIITO	13	48
Asignación Cuentas, Roles y Privilegios SIPLAFT	1	1
Asignación Cuentas, Roles y Privilegios SIVICAL	1	3
Asignación Cuentas, Roles y Privilegios SPARK	3	19
Asignación Cuentas, Roles y Privilegios SVN TORTOISE	1	6
Cambio de vinculación laboral	0	6
Incapacidades por enfermedad o por accidente	5	24
Ingresos de Personal	12	97
Licencias de maternidad o paternidad	2	5
Licencias No remuneradas	2	7
Permisos de personal	3	7
Retiro de personal	17	79
Traslados internos de personal	0	11
Vacaciones de Personal	6	67
Total General	215	1190

Fuente: autores

Figura 12. Ingreso de personal 2016 mantis

Informador:	Monitorizado por:	Asignada a:	Categoría:	Severidad:	Resolución:	Perfil:
Cualquiera	Cualquiera	Cualquiera	Ingresos de Personal	Cualquiera	Cualquiera	Cualquiera
Estado:	Ocultar con Estado:					Prioridad:
Cualquiera	cerrada (Y superiores)					Cualquiera
Ver:	Visibilidad:	Ver Incidencias Fijadas:	Modificadas (hs.):	Usar filtros de fecha:	Relaciones:	
50	Cualquiera	Si	6	No	Cualquiera	
Plataforma:	SO:	Versión de SO:	Etiquetas:			
Cualquiera	Cualquiera	Cualquiera				
calificación						
Cualquiera						
Nota De:	Cualquiera	Ordenadas por:	Actualizada Descendente			
Tipo de coincidencia:	Todas las condiciones					

☐ Buscar
[\[Filtros avanzados \]](#) [\[Crear Enlace Permanente \]](#)

Mostrando Incidencias (1 - 8 / 8) [Imprimir informes] [Exportar a CSV] [Exportar a Excel]

		P	ID	#		Categoría	Severidad	Estado	Actualizada▼	Resumen
<input type="checkbox"/>			0011766	3	1	Ingresos de Personal	mayor	resuelta (eatencio)	01-07-2016	Novedad
<input type="checkbox"/>			0015722	11	1	Ingresos de Personal	mayor	resuelta (vpulgarin)	28-03-2016	Ingresos Planta Coljuegos
<input type="checkbox"/>			0013723	7		Ingresos de Personal	mayor	resuelta (Otorres)	18-12-2015	Ingresos Planta Coljuegos
<input type="checkbox"/>			0012895	10		Ingresos de Personal	mayor	resuelta (Dromero)	09-11-2015	Novedad
<input type="checkbox"/>			0012121	6	4	Ingresos de Personal	mayor	resuelta (ecorredor)	13-10-2015	Novedad
<input type="checkbox"/>			0011914	2	3	Ingresos de Personal	mayor	resuelta (ecorredor)	08-10-2015	Novedades
<input type="checkbox"/>			0009854	2		Ingresos de Personal	mayor	resuelta (eatencio)	14-08-2015	Novedades
<input type="checkbox"/>			0008540	4		Ingresos de Personal	mayor	resuelta (eatencio)	25-06-2015	Novedad

☐ Seleccionar todos

Mover▼

Aceptar

Fuente: autores

Figura 13. Muestra de solicitudes atendidas en el año 2016 sobre gestión de usuarios, roles y privilegios

ID	Informador	Asignada a	Categoría	Fecha de	Actualizac	Resumen	Estado
14721	amontano	fmerchan	Acceso a Carpetas Compartidas	13-01-2016	15-01-2016	ACCESO CARPETAS COMPARTIDAS -	resuelta
14847	amontano	eatencio	Acceso a Carpetas Compartidas	18-01-2016	18-01-2016	INCREMENTO CAPACIDAD CARPETA COMPARTIDA	resuelta
14501	jmolano	ralarcon	Acceso a VPN	04-01-2016	04-01-2016	ORFEO: Usuario temporal ambiente de Producción	cerrada
14789	cortiz	vlargo	Acceso Escritorio remoto de Servidores	15-01-2016	15-01-2016	Proveer acceso de escritorio remoto al señor H	resuelta
15913	vlargo	eatencio	Acceso Escritorio remoto de Servidores	19-02-2016	19-02-2016	Acceso al servidor 10.117.100.28	resuelta
16622	vlargo	eatencio	Acceso Escritorio Remoto de Usuarios	10-03-2016	11-03-2016	Solicitud de autorización de acceso a servidor	resuelta
16621	vlargo	eatencio	Acceso Escritorio Remoto de Usuarios	10-03-2016	29-03-2016	Solicitud de acceso durante tiempo de descanso	resuelta
17679	cocampo	eatencio	Acceso y Permisos a Internet	21-04-2016	02-05-2016	acceso a página de La Previsora	resuelta
16861	Iromero	ralarcon	Acceso y permisos DVD, USB del equipo	17-03-2016	17-03-2016	Solicitud permiso USB	cerrada
16822	Ssoler	dariza	Asignación Cuentas, Roles y Privilegios BD SQL SERVER	16-03-2016	17-03-2016	Creación de usuarios de consulta para atención	resuelta
15925	dariza	eatencio	Asignación Cuentas, Roles y Privilegios INTRANET - CINNOVA	19-02-2016	19-02-2016	Permisos de lectura IP (10.117.100.22)	resuelta
15918	Jzamudio	fmerchan	Asignación Cuentas, Roles y Privilegios INTRANET - CINNOVA	19-02-2016	25-02-2016	Solicitud acceso a intranet de funcionaria Liliana	resuelta
16598	mgallo	ralarcon	Asignación Cuentas, Roles y Privilegios SARA	10-03-2016	10-03-2016	deshabilitación usuario John Jairo Velandia Mc	cerrada
16599	mgallo	ralarcon	Asignación Cuentas, Roles y Privilegios SARA	10-03-2016	10-03-2016	Actualización de Rol cierre de periodo software	cerrada
16046	Iromero	icabrera	Asignación Cuentas, Roles y Privilegios CONTROL ACCESO BIOMETRICO	23-02-2016	28-03-2016	Solicitud acceso Biometrico	resuelta
15919	Jzamudio	icabrera	Asignación Cuentas, Roles y Privilegios CONTROL ACCESO BIOMETRICO	19-02-2016	28-03-2016	Solicitud acceso biométrico funcionaria Liliana	resuelta
16727	Yrozo	fmerchan	Asignación Cuentas, Roles y Privilegios CORREO ELECTRONICO	15-03-2016	18-03-2016	Solicitud correo institucional	resuelta
17507	erubio	fmerchan	Asignación Cuentas, Roles y Privilegios CORREO ELECTRONICO	15-04-2016	20-04-2016	Creación de cuenta	resuelta
15915	ganchila	Otorres	Asignación Cuentas, Roles y Privilegios ELASTIX	19-02-2016	04-03-2016	Configuración perfil	resuelta
15365	amontano	eatencio	Asignación Cuentas, Roles y Privilegios INTERNET	01-02-2016	01-02-2016	SOLICITUD RESTRICCIÓN DE ACCESO A INTERNET	asignada
16988	ralarcon	eatencio	Asignación Cuentas, Roles y Privilegios INTERNET	30-03-2016	30-03-2016	Solicitud Habilitar Internet para poder ver el video	asignada
15908	jcelis	Imendoza	Asignación Cuentas, Roles y Privilegios ISOLUCION	19-02-2016	01-03-2016	Asignación roles a funcionario de la ITRC	resuelta
16263	Imendoza	ralarcon	Asignación Cuentas, Roles y Privilegios ISOLUCION	01-03-2016	01-03-2016	CREACIÓN DE CUENTAS ISOLUCIÓN	cerrada
15809	dariza	eatencio	Asignación Cuentas, Roles y Privilegios MET	16-02-2016	19-02-2016	Permisos lectura ip (10.117.100.57)	resuelta
14509	lpacheco	Idiaz	Asignación Cuentas, Roles y Privilegios ORFEO	04-01-2016	05-01-2016	Solicitud cambio de perfiles de manera temporal	resuelta
14504	cortiz	eatencio	Asignación Cuentas, Roles y Privilegios SIICOL	04-01-2016	05-01-2016	Permiso usuario activo Mario Bucheli	resuelta
14846	bbecerra	fvela	Asignación Cuentas, Roles y Privilegios SIICOL	18-01-2016	18-01-2016	Solicitud asignación de roles en SIICOL	cerrada
17859	ralarcon	dariza	Asignación Cuentas, Roles y Privilegios SIITO	29-04-2016	02-05-2016	Solicitud usuarios y accesos en el servidor 10.117.100.28	cerrada

Fuente: autores

6.2 USO DE HERRAMIENTAS INFORMÁTICAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE ROLES Y PRIVILEGIOS ASIGNADOS A CADA USUARIO EN COLJUEGOS

Las siguientes diapositivas fueron presentadas durante la capacitación realizada a los funcionarios de la oficina de TI el día 16 de agosto de 2016, sobre el modelo para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos, lo cual demuestra la efectividad de dicho modelo.

La figura 14, muestra el uso de la herramienta de mesa de ayuda “mantis” por medio de la cual se crearon las diferentes categorías del proyecto denominado “Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos”. A través de este proyecto, los Jefes de Oficina, Vicepresidentes y Gerentes, envían los requerimientos de asignación de roles y permisos del personal a su cargo.

Figura 14. MANTIS como herramienta para el seguimiento y control de usuarios, roles y privilegios.

Fuente: autores

La figura 15, muestra el uso de la herramienta “Access” por medio de la cual se lleva el control de los usuarios y los sistemas a los cuales se les ha dado permiso. Así, por ejemplo, el usuario Arcila Jiménez Andrea (cuenta aparcala), es un usuario activo y tiene acceso al sistema Orfeo y Siicol. Allí mismo se observa los números de mantis (Número de ticket) u oficio, con el cual fue autorizado por los Jefes de Oficina, Vicepresidentes o Gerentes.

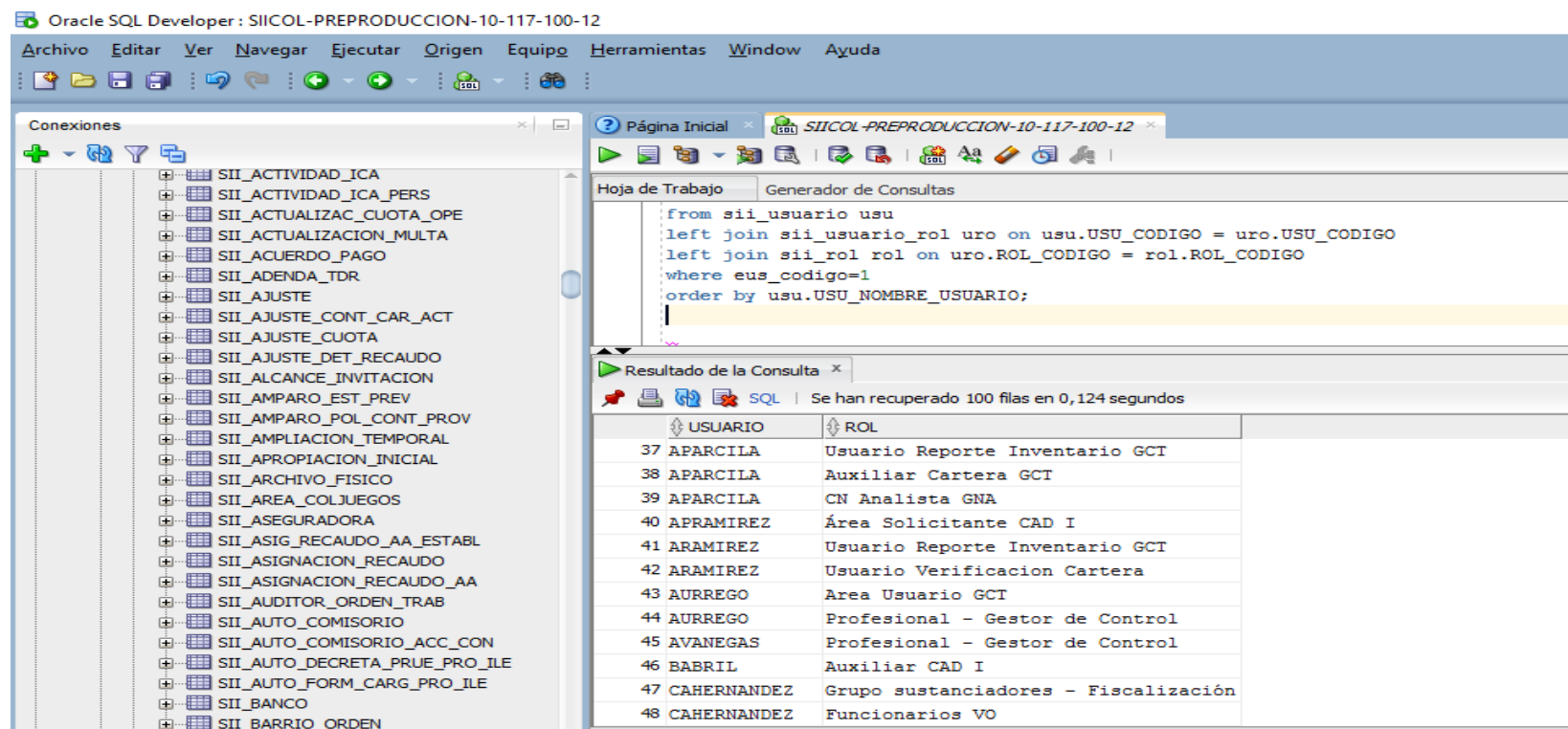
Figura 15. ACCESS como herramienta para el seguimiento y control de usuarios, roles y privilegios.

cuenta	nombre	fecingreso	activo	orfeo	Mantis-AutoOrfeo	siicol	Mantis-AutoSiicol
aparcila	ARCILA JIMENEZ ANDREA DEL PILAR	01/06/2016	SI	SI	18668	SI	18653 y 18670
ITRCEbahamor	BAHAMON TOVAR ERNESTO JIMENO	13/09/2016	SI	SI	20258	SI	20258
ITRCHbarragan	BARRAGAN TORRES HUMBERTO	13/09/2016	SI	SI	20258	SI	20258
Zbayter	BAYTER MARIN ZAMIR	01/10/2015	SI	SI	20602	SI	20162000015403, 20602
Sbeltran	BELTRAN BEJARANO SONIA ESPERANZA	12/02/2016	SI	SI	19074	SI	17209, 18674
ablanc	BLANCO RODRIGUEZ ANGELICA	03/11/2015	NO	NO	20723, 21149	NO	17209, 19576, 21149
Dbuitrago	BUITRAGO CARRILLO DANIEL OSWALDO	16/12/2015	SI	SI	20771	SI	17209, 18674, 20771
Dcasarrubia	CASARRUBIA CONDE DIANA CAROLINA	17/06/2016	SI	SI	19013	SI	19014
Hcollazos	COLLAZOS JOJOA HENRY	10/11/2015	SI	SI	19074	SI	20597
ecorredor	CORREDOR VARGAS EDISSON CAMILO	05/02/2013	NO	NO	19512	NO	19512
Vcortes	CORTES MADARRIAGA VLADIMIR	01/10/2015	NO	NO	21146	NO	17209, 21146
Dgescobar	ESCOBAR ALARCON DIEGO GERMAN	07/07/2016	SI	SI	19328	SI	19329
Gfernandez	FERNÁNDEZ RODRÍGUEZ GINA PAOLA	01/12/2015	NO	NO	20429	NO	17209, 20429
cfierro	FIERRO SEQUERA CARLOS ENRIQUE	28/09/2012	SI	SI	19830	SI	20162000015403
Nfonseca	FONSECA BURGOS NATHALI ALEJANDRA	18/02/2016	SI	SI	19074	SI	18747
sgarcia	GARCIA SUAREZ SERGIO ALEJANDRO	01/10/2015	NO	NO	19735	NO	20162000015403, 19735
Lgomez	GOMEZ GUERRERO LUIS ALFREDO	03/10/2016	SI	SI	20542	SI	20542
Iguerrero	GUERRERO SANTAMARIA LUZ ELENA	26/12/2012	SI	SI	20615, 21183	SI	20162000015403
Lmartinez	MARTINEZ CALLE LUZ HELENA	04/05/2015	NO	NO	21148	NO	20161000013163, 21148
omendez	MENDEZ SOTO OMAR FERNANDO	09/01/2013	SI	SI	19153	SI	20161100107071
smonroy	MONROY JIMENEZ SANDRA CAROLINA	27/11/2012	SI	SI	18915	SI	99991200017513, 18715
Amoreno	MORENO REYES ANDRES ESTEBAN	01/10/2015	NO	NO	18331	NO	18331
Mmoreno	MORENO RODRIGUEZ MARIA DEL PILAR	24/10/2016	SI	SI	20850	SI	20904
Dmorris	MORRIS SALCEDO DIEGO FERNANDO	06/05/2015	NO	NO	19758	NO	20164000013943, 19758

Fuente: autores

La figura 16, muestra el uso de la herramienta “SQL DEVELOPER” por medio de la cual se extrae de las bases de datos ORACLE, los roles y permisos asignados por el líder funcional a cada usuario y a cada aplicación. Así, por ejemplo, el usuario Arcila Jiménez Andrea (cuenta aparcila), le fueron asignados los siguientes tres roles en el sistema SIICOL: “Usuario reporte inventario GCT”, “Auxiliar cartera GCT” y “CN Analista GNA”, los cuales serán verificados con los permisos que le fueron autorizados por los Jefes de Oficina, Vicepresidentes y Gerentes.

Figura 16. SQL ORACLE como herramienta para el seguimiento y control de usuarios, roles y privilegios.



Fuente: autores

Las figuras 17 y 18, muestra el uso de la herramienta "SQL DEVELOPER" por medio de la cual se extrae de las bases de datos SQL SERVER, los roles y permisos asignado por el líder funcional a cada usuario y a cada aplicación. Así, por ejemplo, se observa en la gráfica 17 los diferentes perfiles para la aplicación SIITO y en la gráfica 18 los perfiles asignados a cada usuario, los cuales serán verificados con los permisos que le fueron autorizados por los Jefes de Oficina, Vicepresidentes y Gerentes.

Figura 17. SQL SERVER parte A, como herramienta para el seguimiento y control de usuarios, roles y privilegios.

The screenshot shows the Oracle SQL Developer interface. On the left, the 'Conexiones' (Connections) pane displays a tree structure of database objects, including tables like SIITO_MOV_CARGUE_INVENTARIO, SIITO_MOV_CARGUE_VENTAS, and SIITO_PERFIL. The 'SIITO_PERFIL' table is selected. On the right, the 'Datos' (Data) tab shows the contents of the SIITO_PERFIL table. The table has two columns: PERF_CODIGO and PERF_DESCRIPCION. The data is organized into 21 rows, each representing a different user profile or role.

	PERF_CODIGO	PERF_DESCRIPCION
1		1 ADMINISTRADOR
2		2 OPERADOR REGISTRADO
3		3 FUNCIONARIO
4		4 ADMIN SIITO
5		5 ADMIN SIPLAFT
6		6 ADMIN SCAFO
7		11 COORDINADOR SERVICIO AL CLIENTE
8		12 COORDINADOR DESARROLLO MERCADOS
9		13 ANALISTA SERVICIO AL CLIENTE
10		14 ANALISTA DESARROLLO MERCADOS
11		15 OPERADOR EN REGISTRO
12	10015	OPERADOR_NO_VIGENTE
13	10017	OPERADOR PENDIENTE REGISTRO
14	10018	OPERADOR PENDIENTE CAMBIO CONTRASEÑA
15	10019	OPERADOR PENDIENTE ACTUALIZAR DATOS
16	10020	COORDINADOR FINANCIERO
17	10021	ANALISTA FINANCIERO
18	10022	ANALISTA CALIDAD
19	10024	CONTROL ILEGALIDAD
20	10025	OFICIAL CUMPLIMIENTO SIPLAFT
21	10026	OP ACTUALIZAR

Fuente: autores

Figura 18. SQL SERVER parte B, como herramienta para el seguimiento y control de usuarios, roles y privilegios.

Oracle SQL Developer : SQL_SERVER_UNE10-158-77-5

Archivo Editar Ver Navegar Ejecutar Origen Equipo Herramientas Window Ayuda

Conexiones

- SIITO_REP_MET_VENTAS_DIARIAS_MODIF
- SIITO_REPORTES_PARAM
- SIITO_REQUERIMIENTO
- SIITO_SOLICITUD
- SIITO_SOLICITUD_NOVEDAD
- SIITO_STADO_MOV_SOL
- SIITO_TIP_APUE_TIP_INST
- SIITO_TIP_FAB_PER
- SIITO_TIPO_APLICACION
- SIITO_TIPO_CERTIFICACION
- SIITO_TIPO_DOCUMENTO
- SIITO_TIPO_FABRICANTE
- SIITO_TIPO_PERSONA
- SIITO_TIPO_SOLICITUD
- SIITO_TIPO_UBICACION
- SIITO_TRANSA_NOVEDAD
- SIITO_TRANSACCIONES_NOVEDAD
- SIITO_UBICACION
- SIITO_USUARIO
 - USU_LOGIN
 - USU_PASSWORD
 - USU_SALT
 - USU_CODIGO
 - PERF_CODIGO
 - USU_ESTADO
 - USU_ULTIMO_INICIO_SES
 - USU_TOKEN
 - USU_EMAIL

Página Inicial x SQL_Server_Coljuegos_10-117-100-3 x SQL_SERVER_UNE10-158-77-5 x SIITO_USUARIO x

SQL_SERVER_UNE10-158-77-5

Hoja de Trabajo Generador de Consultas

```
select u.usu_login,u.usu_codigo, u.usu_estado, p.perf_descripcion from DB_SIITO.dbo.siito_usuario U, db_siito.dbo.siito_perfil P
where u.perf_codigo=p.perf_codigo order by u.usu_login
```

Resultado de la Consulta x

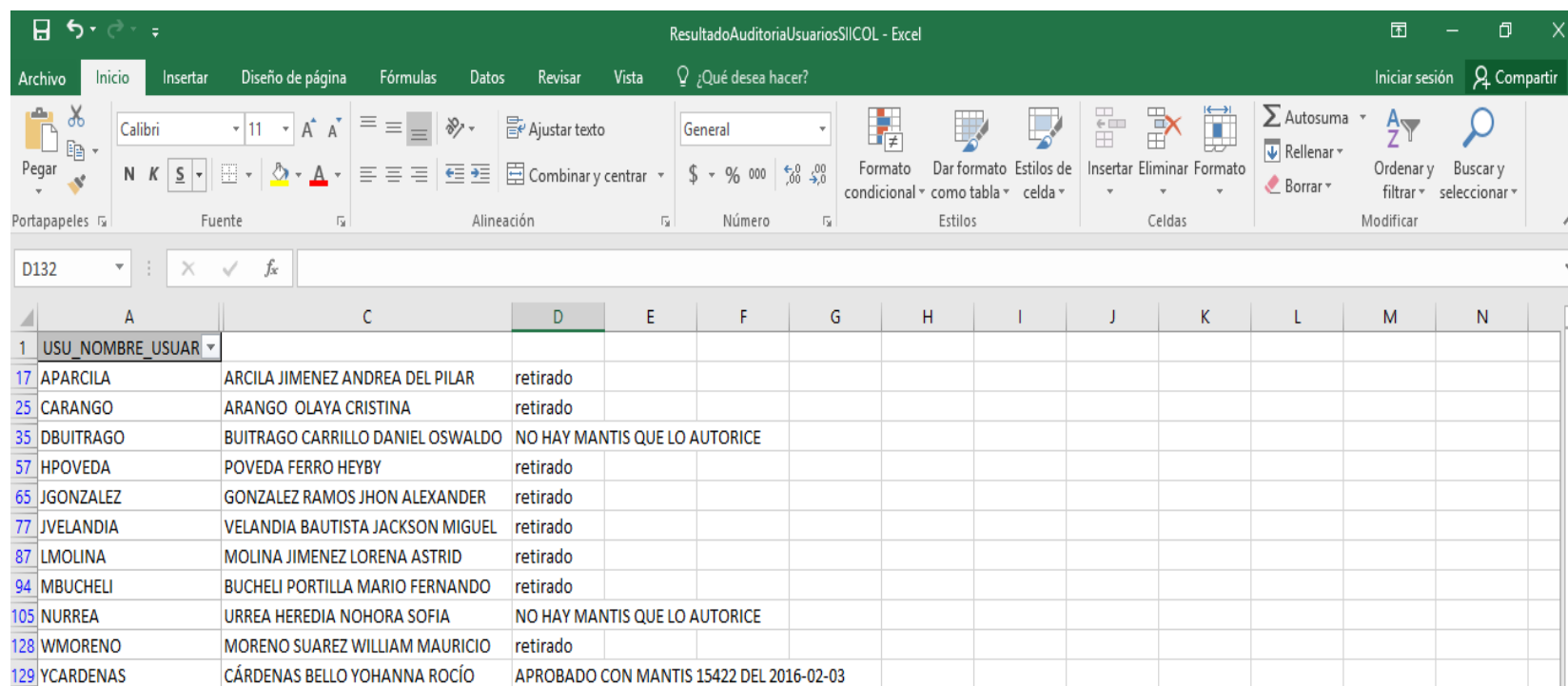
SQL | Se han recuperado 700 filas en 0,063 segundos

usu_login	usu_codigo	usu_estado	perf_descripcion
506 despinosa	51225	true	REPORTES_MET
507 dprieto	61229	true	REPORTES_CONTADORES
508 dramirez	51189	true	ANALISTA FINANCIERO
509 drobayo	51181	true	REPORTES_MET
510 drueda	20209	false	ANALISTA SERVICIO AL CLIENTE
511 DT901003765	51204	true	OPERADOR REGISTRADO
512 edgarperra	20249	true	OPERADOR PENDIENTE REGISTRO
513 emerchan	51139	true	REPORTES_CONTADORES
514 ER900923961	61231	false	OPERADOR PENDIENTE REGISTRO
515 evillalba	51190	false	REPORTES_CONTADORES
516 feslait	30279	false	ANALISTA CALIDAD
517 gcanchila	40305	true	COORDINADOR SERVICIO AL CLIENTE
518 gescobar	20210	true	ANALISTA SERVICIO AL CLIENTE
519 GNA830053023	40296	false	OP_ACTUALIZAR

Fuente: autores

La figura 19, muestra el uso de la herramienta “EXCEL” por medio del cual, y con base a la información extractada sobre los usuarios, roles y permisos de las bases de datos SQL SERVER y ORACLE y con la información de usuarios, roles y permisos que fueron autorizados mediante el software de mesa de ayuda, por los Jefes de Oficina, Vicepresidentes y Gerentes, se realiza el respectivo cruce de información y se obtienen los resultados de las auditorías practicadas.

Figura 19. EXCEL como herramienta para el seguimiento y control de usuarios, roles y privilegios.



	A	C	D	E	F	G	H	I	J	K	L	M	N
1	USU_NOMBRE_USUAR												
17	APARCILA	ARCILA JIMENEZ ANDREA DEL PILAR	retirado										
25	CARANGO	ARANGO OLAYA CRISTINA	retirado										
35	DBUITRAGO	BUITRAGO CARRILLO DANIEL OSWALDO	NO HAY MANTIS QUE LO AUTORICE										
57	HPOVEDA	POVEDA FERRO HEYBY	retirado										
65	JGONZALEZ	GONZALEZ RAMOS JHON ALEXANDER	retirado										
77	JVELANDIA	VELANDIA BAUTISTA JACKSON MIGUEL	retirado										
87	LMOLINA	MOLINA JIMENEZ LORENA ASTRID	retirado										
94	MBUCHELI	BUCHELI PORTILLA MARIO FERNANDO	retirado										
105	NURREA	URREA HEREDIA NOHORA SOFIA	NO HAY MANTIS QUE LO AUTORICE										
128	WMORENO	MORENO SUAREZ WILLIAM MAURICIO	retirado										
129	YCARDENAS	CÁRDENAS BELLO YOHANNA ROCÍO	APROBADO CON MANTIS 15422 DEL 2016-02-03										

Fuente: autores

6.3 AUDITORIAS Y CONSULTAS QUE FACILITAN EL SEGUIMIENTO Y CONTROL DE USUARIOS, ROLES Y PRIVILEGIOS

Las siguientes auditorias y consultas, fueron presentadas durante la capacitación realizada a los funcionarios de la oficina de TI el día 16 de agosto de 2016, sobre el modelo para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos, lo cual demuestra la efectividad de dicho modelo.

- ¿Cuáles funcionarios se han retirado de la empresa y aún siguen activos en los sistemas de información?
- ¿Cuáles funcionarios están activos en los sistemas de información sin tener autorización para ello?
- ¿Cuáles funcionarios tienen más permisos de los autorizados en cada uno de los sistemas de información?
- ¿Cuáles funcionarios tienen un rol determinado en un sistema en particular?
- Un funcionario en particular ¿qué roles tiene asignados en cada uno de los sistemas?
- Durante el año 2015 y 2016 se han realizado auditorias sobre los sistemas SIICOL, SIITO, SIPLAFT, MET, ORFEO y MANTIS e informados a la Jefatura de la OTI.

7. CONCLUSIONES

El modelo implementado para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información, ha permitido:

- Contribuir al cumplimiento de la legislación colombiana (*logs* como mensajes de prueba -ley 527-art 10,11 y 12, Ley 1273-2009-DelitosInformaticos-protección de la información y de los datos, Ley-1581-de-2012-ProteccionDatosPersonales, Ley 1266 de 2008 protección de datos de carácter financiero, crediticio, comercial y de servicios, toda vez que en el evento de una investigación de la violación de estas normas, se cuenta con la traza de la administración de usuarios, roles y privilegios asignados a cada sistema de información.
- Contribuir al mejoramiento de la confidencialidad e integridad de la información en Coljuegos, toda vez que en el año 2015 no se contaba con un sistema para el seguimiento y control de la administración de usuarios, roles y privilegios asignados en los diferentes sistemas de información de Coljuegos, pero con la implementación de este modelo, para junio de 2016 ya se contaba con 215 solicitudes, tal como lo muestra la Tabla 2. Número de solicitudes atendidas en el año 2016 sobre gestión de usuarios, roles y privilegios y para noviembre 16 de 2016 se incrementaron este tipo de solicitudes a 1.190.
- Aumentar la confianza de los usuarios evitando vulnerabilidades derivadas de accesos indebidos por parte de usuarios.
- Mejorar el seguimiento, control y traza de la administración de usuarios, roles y privilegios asignados a cada sistema de información
- Facilitar el desarrollo de auditorías al respecto

Las actividades realizadas para la administración de usuarios, roles y privilegios, han permitido mejorar la seguridad de la información en Coljuegos y más específicamente al establecimiento de los siguientes controles establecidos en la norma ISO 27001:

- Política de control del acceso
- Registro de usuarios
- Gestión de privilegios

- Gestión de contraseñas para usuarios
- Revisión de los derechos de acceso de los usuarios
- Uso de contraseñas
- Procedimiento de ingreso seguro
- Identificación y autenticación de usuarios
- Sistema de gestión de contraseñas
- Tiempo de inactividad de la sesión
- Restricción del acceso a la información
- Fuga de Información
- Controles de auditoría de los sistemas de información
- Acuerdos sobre confidencialidad
- Retiro de los derechos de acceso

BIBLIOGRAFÍA

ACTUALICESE.COM. ¿Qué es auditoría? Recuperado el 23 de agosto de 2016 de: actualicese.com › Revisoría Fiscal, Auditoría y Control

BOGOTATURISMO. Norma Técnica Colombiana NTC-ISO/IEC 27001. Recuperado el 02 de octubre de 2016 en: <http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf>

COLJUEGOS. ¿Qué es Siplaft? Recuperado el 23 de agosto de 2016 en: www.coljuegos.gov.co/publicaciones/300493

_____. Sistema Integrado de Información de Coljuegos. Recuperado el 23 de agosto de 2016 en: www.coljuegos.gov.co/descargar.php?idFile=215916

_____. Coljuegos. Recuperado el 02 de agosto de 2016 de: <http://www.coljuegos.gov.co/loader.php?IServicio=Glosario&letra=C>

_____. Sabes que es el ITRC. Recuperado el 02 de octubre de 2016 de: <file:///C:/Users/sistemas01/Downloads/ITRC.pdf>

_____.; Requerimientos Técnicos Sistema Conexión en Línea Máquinas Electrónicas Tragamonedas SCLM. Recuperado el 02 de octubre de 2016 de: www.coljuegos.gov.co/descargar.php?idFile=216213

DC.UBA. Definición de permiso. Recuperado el 02 de octubre de 2016 en: http://www-2.dc.uba.ar/materias/seginf/material/Clase02-Unidad2_vf.pdf

DIALNET. Qué son líderes funcionales. Recuperado el 23 de agosto de 2016 de: <https://dialnet.unirioja.es/descarga/articulo/4895442.pdf>

EL MUNDO DE LAS TICS. Gestión de mesa de ayuda. Recuperado el 02 de octubre de 2016 de: http://www.elmundodelastics.net/2008/10/la-funcin-de-una-mesa-de-ayuda-en-los.html#.V_Vwfo_hCUk

EVOLUTION-IT. Ingeniería de roles. Recuperado el 02 de octubre de 2016 de: <http://www.evolution-it.com.co/portafolio/gestion-de-la-seguridad/ingenieria-de-roles.html>

GERENCIE. Sistemas de información. Recuperado el 23 de agosto de 2016 en: www.gerencie.com/sistemas-de-información

_____. Qué es personería jurídica. Recuperado el 23 de agosto de 2016 en: gerencie.com/persona-juridica.html

GOOGLE DOCS. Gestión de Usuarios. Recuperado el 02 de octubre de 2016 de: https://docs.google.com/document/d/1wyg6NbMoiFEg6lZZ_POBZFx7ly3fx3xPcpQ8olcMXiQ/edit

HERNÁNDEZ MOLINA, Ignacio. La formulación de proyectos en ciencias e ingenierías. Bogotá D.C.: Universidad Piloto de Colombia. 2015. 274p.

IBM. Cuentas huérfanas. Recuperado el 02 de octubre de 2016 de: http://www.ibm.com/support/knowledgecenter/es/SSTFWV_5.1.0/com.ibm.itim.doc/ref/ref_ic_reportspack_orphan_account.html

ID MANAGEMENT. Gestión de identidades. Recuperado el 23 de agosto de 2016 de: [Search datacenter.techtarget.com/es/definicion/Gestion-de-identidades-ID-management](http://search.datacenter.techtarget.com/es/definicion/Gestion-de-identidades-ID-management)

INCIBE. Plan de Contingencia y Continuidad de Negocio. Recuperado el 02 de octubre de 2016 de: <https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio>

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Normas Colombianas para documentación, presentación de tesis, trabajos de grado, y otros trabajos de investigación. Sexta actualización. Bogotá D.C.: ICONTEC, 2008. 41p. NTC 1486.

INSTITUTO DE TECNOLOGIA DE MASSACHUSETTS. Capítulo 13. Protocolo ligero de acceso a directorios (LDAP). Recuperado el 02 de octubre de 2016 de: web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ldap.html

INTEGRATE ACCESS MANAGEMENT. ¿Qué es gestión de Identidad y Acceso (IAM)? Recuperado el 23 de agosto de 2016 de: www.gartner.com/it/identity-and-access-management-iam

ISEGORIA. ¿Qué es sujeto? Recuperado el 23 de agosto de 2016 en: [isegoria revistas.csic.es/index.php/isegoria/article/viewFile/95/95](http://isegoria.revistas.csic.es/index.php/isegoria/article/viewFile/95/95)

ISO 27000. Política y objetivos de seguridad. Recuperado el 02 de octubre de 2016 en: http://www.iso27000.es/download/doc_sgsi_all.pdf

MANTISBT. Mantis. Recuperado el 02 de octubre de 2016 de <https://www.mantisbt.org/>

MICROSOFT. ¿Qué son directorios virtuales? Recuperado el 23 de agosto de 2016 de: <https://support.microsoft.com/es-co/kb/142853>

MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. ¿Qué es canal PQRD?: Recuperado el 23 de agosto de 2016 de: www.mintic.gov.co

_____. Confidencialidad. Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

_____. Disponibilidad. Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

_____. Integridad. Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

_____. TIC para el desarrollo. Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

_____. Usuario (UIT-T Rec M.60 (93)). Recuperado el 02 de octubre de 2016 de: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

MONTOYA S., José A. y RESTREPO R., Zuleima. Gestión de identidades y control de acceso desde una perspectiva organizacional. Artículo, Vol. 3 No. 1, Medellín, 2012.

MUÑOZ RAZO, Carlos. Auditoría en sistemas computacionales. Primera edición. México: Prentice hall. 2002. 796p

ORFEOLIBRE. Orfeo sistema de gestión documental. Recuperado el 02 de octubre de 2016 en: <http://www.orfeolibre.org/portal/>

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO 27001. Recuperado el 23 de agosto de 2016 de: www.iso.gov.co

PROFESORES.FI. ¿Que es objeto? Recuperado el 02 de agosto de 2016 en: http://profesores.fi-b.unam.mx/carlos/aydoo/conceptos_oo.html

PROSPERIDAD SOCIAL. Política corporativa de gobierno de identidad. Recuperado el 23 de agosto de 2016 en: www.prosperidadsocial.gov.co/.../Manual%20de%20Identidad%20Corporativa%20Pr...

RECURSOSTIC. Mecanismos básicos de seguridad. Recuperado el 02 de octubre de 2016 de:

<http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=2>

REDCIENTIFICA. Conceptos de gestión de privilegios y recursos. Recuperado el 02 de octubre de 2016 en: <http://www.redcientifica.com/oracle/c0004p0004.html>

REDIRIS. Servicios de directorios. Recuperado el 23 de agosto de 2016 en: <https://www.rediris.es/ldap/doc/ldap-intro.pdf>

SEGU-INFO. Seguridad Lógica – Identificación y Autenticación. Recuperado el 02 de octubre de 2016 de: <http://www.segu-info.com.ar/logica/identificacion.htm>

SUPERSU. ¿Qué es súper usuario? Recuperado el 23 de agosto de 2016 en: supersu.uptodown.com/android

UDEA. Las Entidades Descentralizadas. Recuperado el 02 de octubre de 2016 de: http://docencia.udea.edu.co/derecho/constitucion/eje_conform_entidades_desc.html

UNIVERSIDAD DE CHILE. Introducción a los conceptos básicos de la Teoría General de Sistemas. Recuperado el 02 de octubre de 2016 de www.facso.uchile.cl/publicaciones/moebio/03/frprinci.htm

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Definición de No repudio. Recuperado el 23 de agosto de 2016 en: redyseguridad.fip.unam.mx/proyectos/seguridad/ServNoRepudio.php

UNIVERSIDAD TÉCNICA DE MANAUBI. ¿Qué es UTM? Recuperado el 23 de agosto de 2016 en: www.utm.edu.ec/

UNIVERSO JUS. Definición de Autonomía Administrativa. Recuperado el 23 de agosto de 2016 de: universojus.com/definición/autonomía-administrativa

VILLALOBOS BECERRA, Refugio Javier. Propuesta de arquitectura de gestión de identidades digitales para el consorcio minero Benito Juárez Peña Colorada, tesis de grado, Universidad de Colima, 2012.

WHATLS. ¿Qué es continuidad de negocio? Recuperado el 23 de agosto de 2016 de: [Search data center.techtarget.com/es/definicion/Continuidad-de-negocios-BC](http://searchdatacenter.techtarget.com/es/definicion/Continuidad-de-negocios-BC)

WORDPRESS. Definición de gestión de roles. Recuperado el 23 de agosto de 2016 de: <https://coleccion.wordpress.com/category/moodle/gestion-de-roles/>

_____. Metadirectorios. Recuperado el 23 de agosto de 2016 de:
<https://buscadores en espanol.wordpress.com/tag/metadirectorios>

ANEXOS

ANEXO A. ROLES Y PRIVILEGIOS DE LAS APLICACIONES

ROLES, MÓDULOS Y PERMISOS ORFEO

La seguridad para el manejo de la información en ORFEO, se hace de la siguiente manera: Primero al funcionario se le asigna uno de los siguientes roles mostrados en el cuadro de roles (cuadro 5) y posteriormente se le asigna los permisos que se consideren y que se encuentran definidos en el cuadro de permisos (cuadro 6).

Cuadro 5. Roles ORFEO

Grupo de usuarios	Descripción del grupo
Administrador	Permite ingresar, consultar, modificar, crear y actualizar información de los siguientes módulos: Administración, envíos, impresión, anulación, TRD, Remitentes y terceros, consultas, archivo, devolución de correo, radicación y administración de carpetas.
Canal de Distribución	Permite usar los siguientes módulos: Impresión (ingresar, consultar y actualizar), anulación (ingresar, consultar y crear), TRD (ingresar y consultar), Remitentes y terceros (ingresar y consultar), consultas (ingresar y consultar), archivo (ingresar y consultar), devolución de correo (ingresar, consultar y crear), radicación (ingresar, consultar y actualizar) y administración de carpetas (ingresar, consultar y crear).
Canal PQRD	Permite usar los siguientes módulos: Consultas (Ingresar y consultar), archivo (ingresar y consultar) y radicación (ingresar, consultar, crear y actualizar).
Usuario Normal	Permite ingresar y consultar información en los siguientes módulos: Remitentes y terceros (Ingresar y consultar), Consultas (ingresar y consultar), Archivo (ingresar y consultar), Devolución de correo (ingresar y consultar), radicación (ingresar y consultar), administración carpetas (ingresar y consultar).

Fuente: autores

Cuadro 6. Permisos ORFEO

Módulo	Permisos
Digitalización de Documentos	(0) No tiene permiso asignado (1) puede asociar la imagen en radicados que no la tengan (2) puede asociar la imagen en radicados que ya tengan una asociada
Modificaciones	Permite realizar modificaciones sobre los radicados
Impresión	(0) No tiene permiso asignado (1) Puede marcar documentos como impresos generados únicamente en su dependencia (2) Puede marcar documentos como impresos generados en cualquier dependencia
Solicitud de Anulaciones	Permite solicitar la anulación de un radicado cuando existan errores en la radicación con la respectiva justificación
Administrador de Archivo	(0) No tiene permiso asignado (1) Puede archivar documentos en los diferentes almacenamientos parametrizados dentro del sistema (2) Puede realizar la administración, creación y edición de los tipos de almacenamiento y puede archivar documentos
Administrador del Sistema	Usuario con permisos para realizar la parametrización en Orfeo en todos sus ambientes
Usuario Reasigna	Permite que un usuario normal pueda realizar la reasignación de los radicados a un jefe de otra dependencia sin pasar por su jefe inmediato
Usuario Activo	Se establece que un usuario está activo o no en el sistema. Cuando un usuario se desactiva se cierra el usuario y por lo tanto no se le pueden asignar ningún tipo de radicado
Usuario Nuevo	Indica que el usuario que se crea es nuevo, para que en el momento de ingresar por primera vez a Orfeo el sistema lo reconozca y Orfeo le solicite el cambio de clave
Puede Archivar Documentos	Permite realizar el archivo virtual de cualquier radicado generado en Orfeo a la Dependencia final

Continuación Cuadro 6. Permisos ORFEO

Módulo	Permisos
Creación de expedientes	(0) No puede crear expedientes (1) Permiso para crear expedientes virtuales (2) Puede crear expedientes virtuales y cambiar el responsable de un expediente
Remitentes / Terceros	Remitentes / Terceros
Tablas de Retención Documental	Administración del módulo de tablas de retención documental que permite el mantenimiento y parametrización de las series, sub-series y tipos documentales asignándoles el tiempo
Radicación Masiva	Permite generar varias cartas de salida, memorando o cualquier tipo de radicación con una plantilla creada previamente por el usuario, que contiene el mismo texto y serán remitidas a diferentes destinatarios.
Préstamo de Documentos	Permite el registro y control de los documentos físicos que son radicados en Orfeo y que requieren realizar el préstamo del documento a cualquier usuario de la entidad para una consulta temporal
Anulaciones	Anulaciones
Devoluciones de Correo	Permite ver los radicados que han sido devueltos al área por la agencia de correo y que deben ser revisados en sus datos de envío para determinar si se realiza nuevamente el envío o no
Envíos de Correo	Permite realizar el registro de los radicados en su proceso final, correspondiente al envío de los documentos que son entregados a las diferentes agencias de correo para su reparto o que se deben enviar internamente
Estadísticas	(0) El usuario solamente podrá visualizar las estadísticas de documentos que él mismo haya realizado (1) Se puede consultar los reportes de todas las personas que pertenecen a la misma área. (2) Puede generar reportes de todos los usuarios del sistema Orfeo sin importar en qué dependencia se encuentren
Nivel de Seguridad	1, 2, 3, 4, 5

Continuación Cuadro 6. Permisos ORFEO

Módulo	Permisos
Firma Digital	(0) Puede realizar la solicitud de firma de documentos (1) Puede realizar la firma Digital a los documentos solicitados (2) Puede realizar la solicitud de firma de documentos y puede realizar la firma a los mismos.
Usuario Público	Permite que un usuario normal de una dependencia X, pueda ser visto por los otros usuarios de una dependencia y le puedan asignar radicados en Orfeo como si el usuario de la dependencia X perteneciera a la dependencia Y
Notificación de Resoluciones	Permite realizar el registro de la notificación de una resolución
Trámite Respuesta Radicado	Permite el mantenimiento y parametrización de las entidades, empresas o personas naturales que remiten documentos a la entidad y reciben documentos de la misma
Radicación Express	(0) No tiene permiso asignado (1) Permiso para radicación rápida (2) Permiso para modificación rápida (3) Permiso para radicación rápida y modificación rápida
(1) Salida	(0) No tiene asignado el permiso (1) Puede radicar desde la sección izquierda de radicación (2) Puede radicar documentos desde la pestaña de documentos (3) Puede radicar por cualquier opción (sección radicación y pestaña de documentos)
(3) Interna	(0) No tiene asignado el permiso (1) Puede radicar desde la sección izquierda de radicación (2) Puede radicar documentos desde la pestaña de documentos (3) Puede radicar por cualquier opción (sección radicación y pestaña de documentos)

Continuación Cuadro 6. Permisos ORFEO

Módulo	Permisos
(9) Históricos	<p>(0) No tiene asignado el permiso</p> <p>(1) Puede radicar desde la sección izquierda de radicación</p> <p>(2) Puede radicar documentos desde la pestaña de documentos</p> <p>(3) Puede radicar por cualquier opción (sección radicación y pestaña de documentos)</p>
Reporte Radicación	Reporte Radicación
(2) Entrada	0, 1
(8) PQRD	<p>(0) No tiene asignado el permiso</p> <p>(1) Puede radicar desde la sección izquierda de radicación</p> <p>(2) Puede radicar documentos desde la pestaña de documentos</p> <p>(3) Puede radicar por cualquier opción (sección radicación y pestaña de documentos)</p> <p>Permite que un usuario pueda borrar los documentos que han sido digitalizados y enviados como anexos a un radicado principal.</p>
Se autentica por medio de LDAP	Indica que el ingreso a Orfeo se hará con la clave del servidor de autenticación de la red de la entidad. Se asignará cuando la Entidad así lo requiera
Puede Asignar Pre-radicado	Puede Asignar Pre-radicado
Puede Tipificar Anexos .tif	Permite la re-tipificación de los anexos digitalizados y que requiere modificar el tipo documental. Se asignará este permiso a un usuario responsable para que pueda tipificar los anexos digitalizados
Puede utilizar el editor de Flujos	Permite realizar la parametrización de los flujos de trabajo con los diferentes estados en los que puede estar un expediente específico, teniendo en cuenta la asignación de la serie y la sub-serie de dicho expediente

Continuación Cuadro 6. Permisos ORFEO

Módulo	Permisos
Resolución	(0) No tiene asignado el permiso (1) Puede radicar desde la sección izquierda de radicación (2) Puede radicar documentos desde la pestaña de documentos (3) Puede radicar por cualquier opción (sección radicación y pestaña de documentos)
Autos	(0) No tiene asignado el permiso (1) Puede radicar desde la sección izquierda de radicación (2) Puede radicar documentos desde la pestaña de documentos (3) Puede radicar por cualquier opción (sección radicación y pestaña de documentos)
Circulares	(0) No tiene asignado el permiso (1) Puede radicar desde la sección izquierda de radicación (2) Puede radicar documentos desde la pestaña de documentos (3) Puede radicar por cualquier opción (sección radicación y pestaña de documentos)

Fuente: autores

ROLES, MÓDULOS Y PERMISOS SIICOL

La seguridad para el manejo de la información en SIICOL, se hace de la siguiente manera: A cada usuario se le asigna un rol (cuadro 7), a su vez al rol se le asigna unos módulos (cuadro 8) y a los módulos se les asigna unos permisos (cuadro 9).

Cuadro 7 Roles SIICOL

Roles
Administrador
Administrador Base de Datos
Administrador Sesiones
Administrador Usuarios
Analista póliza localizados
Aprobador póliza localizados
Área Solicitante CAD I
Área Usuario Cartera
Área Usuario Contratación Adm
Área Usuario DME
Área Usuario DME – GNA
Área Usuario DME – GNN
Área Usuario GCT
Área Usuario Gestión Contable
Área Usuario Presupuesto

Continuación Cuadro 7. Roles SIICOL

Roles
Área Usuario Tesorería
AUDITORIAS ENTES DE CONTROL
Auxiliar CAD I
Auxiliar Cartera GCT
Auxiliar Contable SENA
Auxiliar DME GNA
Auxiliar DME GNN
Auxiliar GCT Marcador
Auxiliar Gestión Contable I
Auxiliar Gestión Contable II
Auxiliar Gestión Contable III
Auxiliar Tesorería
CN Abogado revisor
CN Administrador
CN Analista GNA
CN Canal de distribución
CN Evaluador CCO
CN Evaluador financiero
CN Evaluador GCT
CN Notificaciones SAC
Consultas / Soporte usuario
Control Interno
Ejecutor Manual Procesos Cartera
Jefe Área Solicitante CAD
Jefes Consultas
PR Administrador
PR Analista GNA
PR Notificaciones SAC
Profesional Tesorería
Técnico II Tesorería
Usuario Verificación Cartera

Fuente: autores

Cuadro 8. Módulos SIICOL.

Módulos
Acción de control
Acta de Inicio
Acuerdos de pago
Adendas términos de referencia
Adición Presupuestal
Adjudicación
Administración

Continuación Cuadro 8. Módulos SIICOL.

Módulos
Administración de Recursos Financieros
Alcance invitación proceso selección
Auto comisorio visita
Balance de Prueba
Beneficiarios ET
Carga de Contratos
Cargar Nómina Funcionarios Planta
Cargue Documento CONPES
Cargue Masivo Comprobantes Contables
Cartera
CDP Expedidos
Centros de Costos
Cierre Anual Contable
Cierre Mensual
Cierre recaudo
Conceptos Nómina
Contabilidad
Contratación Administrativa
Contrato de Concesión
Cuenta Contable
Cuentas por pagar
Cuentas Por Pagar Por Edades
Cuentas por Tipo de Movimiento
Decremento CDP
Decremento RP
Cuadro 15 (Continuación)
Denuncias y Hallazgos
Desarrollo de Mercados
Designación supervisor
Distribución
Estado de cuenta Acuerdos de Pago
Estado de cuenta GCT
Estado de cuenta GENERAL
Estudio de Mercado
Estudio Previo
Evaluación de Propuestas
Expedición CDP
Expedir RP masivo nómina
Fuentes de Financiación
Generación de la Minuta

Continuación Cuadro 8. Módulos SIICOL.

Módulos
Generar Obligación Transferencia ET
Generar Orden de Pago Transferencia ET
Gestión Contractual
Ilegalidad
Incremento CDP
Incremento de RP
Informe de supervisión contrato de concesión
Informe verificación en campo
Interés Diario
Invitación proceso de selección
Libro Auxiliar Por Comprobante
Libro Auxiliar Por Rango de Cuentas
Limpieza Caché
Liquidación contrato concesión
Liquidación Mensual
Liquidación Mensual
Marcación inventario no reportado
Modificación CDP
Modificación RP
Nómina
Obligación
Obligación Funcionarios Planta
Obligación No presupuestal
Obligación Transferencia ET
Oficio de Liquidación
Oficio de Liquidación Contrato Nuevo
Oficio de Liquidación Modificación Contrato
Orden de Pago
Orden de Pago Cuentas por Pagar
Orden de pago No presupuestal
Orden de Pago Nómina Funcionarios Planta
Orden de Pago Transferencia ET
Otrosí Contrato de Concesión
PAC y Tesorería
Pago Operadores en Banco
Pago Operadores PSE
Pagos Ejecutados 4xMil
Parámetros
Póliza Contrato Concesión
Póliza Garantía

Continuación Cuadro 8. Módulos SIICOL.

Módulos
Póliza Otrosí Contrato de Concesión
Presupuesto
Procesamiento Contabilidad
Procesamiento cuentas por pagar
Procesamiento Nómina
Proceso sancionatorio
Proveedores
Proyección Flujo de Caja
Reasignación Reparto
Recaudo establecimiento contrato
Recaudo y Transferencia
Recepción de Propuestas
Reducción Presupuestal
Registrar Programación PFC mensual
Registro Aprobación PAC mensual
Registro Apropiación Inicial
Registro Comprobante Contable
Registro de Aprobación PAC
Registro empresas
Registro Presupuestal
Registro Solicitud PFC mensual
Registro Sustanciadores – Fiscalizadores
Registro Traslado Presupuestal
Reintegro pagaduría
Renovación Póliza Contrato de Concesión
Reporte Auxiliar por Operaciones
Reporte Auxiliar por Terceros
Reporte Cadena Presupuestal
Reporte Conciliación Contabilidad – Cartera
Reporte Contrato Concesión
Reporte Ejecución presupuestal de gastos
Reporte Ejecución presupuestal de ingresos
Reporte Histórico De Cuentas Por Pagar
Reporte Inventario Contrato Concesión
Reporte Libro Diario
Reporte Libro Mayor
Reporte Liquidación mensual
Reportes Contabilidad
Reportes gestión contractual
Reportes Liquidación Mensual
Reportes Modificación CDP

Continuación Cuadro 8. Módulos SIICOL.

Módulos
Reportes Modificación RP
Reportes Presupuesto
Resolución Autorización Localizados
Roles
RP Expedidos
Saldo Inicial Cuentas Bancarias
Sesiones Activas
Solicitud autorización de rifas
Solicitud autorización promocionales
Solicitud CDP
Solicitud de Pago
Solicitud Estudio de Mercado
Sql Directo
Suspensión contrato de concesión
Tasas interés Súper-financiera
Terminación Anticipada de Contrato
Términos de referencia
Tipo Comprobante Contable
Tipo Retención
Traslado Entre Cuentas Bancarias
Traslado entre ítems del Plan de contratación
Usuarios
Validación de Interés

Fuente: autores

Cuadro 9. Permisos SIICOL.

Permisos
REGISTRAR
MODIFICAR
BORRAR
IMPRIMIR
APROBAR
RECHAZAR
CONSULTAR
DEVOLVER
REVISAR
GENERAR

Fuente: autores

Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Administrador	Acta de Inicio	S	S	S	S	S	S	S	S	S	S
Administrador	Adendas términos de referencia	S	S	S	S	S	S	S	S	S	S
Administrador	Adición Presupuestal	S	S	S	S	S	S	S	S	S	S
Administrador	Adjudicación	S	S	S	S	S	S	S	S	S	S
Administrador	Administración	S	S	S	S	S	S	S	S	S	S
Administrador	Administración de Recursos Financieros	S	S	S	S	S	S	S	S	S	S
Administrador	Alcance invitación proceso selección	S	S	S	S	S	S	S	S	S	S
Administrador	Balance de Prueba	S	S	S	S	S	S	S	S	S	S
Administrador	Carga de Contratos	S									
Administrador	Cargar Nómina Funcionarios Planta	S	S	S	S	S	S	S	S	S	S
Administrador	Cargue Documento CONPES	S	S	S	S	S	S	S	S	S	S
Administrador	Cartera							S			
Administrador	CDP Expedidos	S	S	S	S	S	S	S	S	S	S
Administrador	Centros de Costos	S	S	S	S	S	S	S	S	S	S
Administrador	Cierre Mensual	S	S	S	S	S	S	S	S	S	S
Administrador	Contratación Administrativa	S	S	S	S	S	S	S	S	S	S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Administrador	Contrato de Concesión	S	S	S	S	S	S	S	S	S	S
Administrador	Cuentas por pagar							S			
Administrador	Decremento CDP	S	S	S	S	S	S	S	S	S	S
Administrador	Decremento RP	S	S	S	S	S	S	S	S	S	S
Administrador	Desarrollo de Mercados	S	S	S	S	S	S	S	S	S	S
Administrador	Designación supervisor	S	S	S	S	S	S	S	S	S	S
Administrador	Estado de cuenta Acuerdos de Pago	S	S	S	S	S	S	S	S	S	S
Administrador	Estado de cuenta GCT	S	S	S	S	S	S	S	S	S	S
Administrador	Estado de cuenta GENERAL	S	S	S	S	S	S	S	S	S	S
Administrador	Estudio de Mercado	S	S	S	S	S	S	S	S	S	S
Administrador	Estudio Previo	S	S	S	S	S	S	S	S	S	S
Administrador	Evaluación de Propuestas	S	S	S	S	S	S	S	S	S	S
Administrador	Expedición CDP	S	S	S	S	S	S	S	S	S	S
Administrador	Fuentes de Financiación	S	S	S	S	S	S	S	S	S	S
Administrador	Generación de la Minuta	S	S	S	S	S	S	S	S	S	S
Administrador	Generar Obligación Transferencia ET	S	S	S	S	S	S	S	S	S	S
Administrador	Gestión Contractual	S	S	S	S	S	S	S	S	S	S
Administrador	Incremento CDP	S	S	S	S	S	S	S	S	S	S
Administrador	Invitación proceso de selección	S	S	S	S	S	S	S	S	S	S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Administrador	Libro Auxiliar Por comprobante	S	S	S	S	S	S	S	S	S	S
Administrador	Libro Auxiliar Por Rango de Cuentas	S	S	S	S	S	S	S	S	S	S
Administrador	Limpieza Caché	S									
Administrador	Liquidación Mensual							S			
Administrador	Marcación inventario no reportado	S	S	S	S	S	S	S	S	S	S
Administrador	Modificación CDP	S	S	S	S	S	S	S	S	S	S
Administrador	Modificación RP	S	S	S	S	S	S	S	S	S	S
Administrador	Nómina							S			
Administrador	Obligación	S	S	S	S	S	S	S	S	S	S
Administrador	Obligación Funcionarios Planta	S	S	S	S	S	S	S	S	S	S
Administrador	Obligación No presupuestal	S	S	S	S	S	S	S	S	S	S
Administrador	Obligación Transferencia ET	S	S	S	S	S	S	S	S	S	S
Administrador	Oficio de Liquidación	S	S	S	S	S	S	S	S	S	S
Administrador	Oficio de Liquidación Contrato Nuevo	S	S	S	S	S	S	S	S	S	S
Administrador	Oficio de Liquidación Modificación Contrato	S	S	S	S	S	S	S	S	S	S
Administrador	Orden de Pago	S	S	S	S	S	S	S	S	S	S
Administrador	Orden de Pago Cuentas por Pagar	S	S	S	S	S	S	S	S	S	S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Administrador	Orden de Pago Funcionarios Planta	S	S	S	S	S	S	S	S	S	S
Administrador	Orden de pago No presupuestal	S	S	S	S	S	S	S	S	S	S
Administrador	Orden de Pago Nómina Funcionarios Planta	S	S	S	S	S	S	S	S	S	S
Administrador	PAC y Tesorería	S	S	S	S	S	S	S	S	S	S
Administrador	Pago Operadores en Banco	S	S	S	S	S	S	S	S	S	S
Administrador	Parámetros							S			
Administrador	Póliza Contrato Concesión	S	S	S	S	S	S	S	S	S	S
Administrador	Póliza Garantía	S	S	S	S	S	S	S	S	S	S
Administrador	Presupuesto	S	S	S	S	S	S	S	S	S	S
Administrador	Procesamiento Contabilidad							S			
Administrador	Procesamiento cuentas por pagar							S			
Administrador	Procesamiento Nómina							S			
Administrador	Proveedores	S	S	S	S	S	S	S	S	S	S
Administrador	Proyección Flujo de Caja	S	S	S	S	S	S	S	S	S	S
Administrador	Recaudo y Transferencia	S	S	S	S	S	S	S	S	S	S
Administrador	Recepción de Propuestas	S	S	S	S	S	S	S	S	S	S
Administrador	Reducción Presupuestal	S	S	S	S	S	S	S	S	S	S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Administrador	Registro Aprobación PAC mensual	S	S	S	S	S	S	S	S	S	S
Administrador	Registro Apropriación Inicial	S	S	S	S	S	S	S	S	S	S
Administrador	Registro Comprobante Contable	S	S	S	S	S	S	S	S	S	S
Administrador	Registro de Aprobación PAC	S	S	S	S	S	S	S	S	S	S
Administrador	Registro Presupuestal	S	S	S	S	S	S	S	S	S	S
Administrador	Registro Solicitud PFC mensual	S	S	S	S	S	S	S	S	S	S
Administrador	Registro Traslado Presupuestal	S	S	S	S	S	S	S	S	S	S
Administrador	Reporte Auxiliar por Operaciones	S	S	S	S	S	S	S	S	S	S
Administrador	Reporte Auxiliar por Terceros	S	S	S	S	S	S	S	S	S	S
Administrador	Reporte Cadena Presupuestal	S	S	S	S	S	S	S	S	S	S
Administrador	Reporte Contrato Concesión	S	S	S	S	S	S	S	S	S	S
Administrador	Reporte Ejecución presupuestal de gastos	S	S	S	S	S	S	S	S	S	S
Administrador	Reporte Inventario Contrato Concesión	S	S	S	S	S	S	S	S	S	S
Administrador	Reporte Liquidación mensual	S	S	S	S	S	S	S	S	S	S
Administrador	Reportes Contabilidad							S			
Administrador	Reportes gestión contractual							S			
Administrador	Reportes Liquidación Mensual							S			
Administrador	Reportes Presupuesto	S	S	S	S	S	S	S	S	S	S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Administrador	Resolución Autorización Localizados	S	S	S	S	S	S	S	S	S	S
Administrador	Roles	S	S	S	S	S	S	S	S	S	S
Administrador	RP Expedidos	S	S	S	S	S	S	S	S	S	S
Administrador	Saldo Inicial Cuentas Bancarias	S	S	S	S	S	S	S	S	S	S
Administrador	Sesiones Activas	S	S	S	S	S	S	S	S	S	S
Administrador	Solicitud CDP	S	S	S	S	S	S	S	S	S	S
Administrador	Solicitud de Pago	S	S	S	S	S	S	S	S	S	S
Administrador	Solicitud Estudio de Mercado	S	S	S	S	S	S	S	S	S	S
Administrador	Tasas interés Súper financiera	S	S	S	S	S	S	S	S	S	S
Administrado	Términos de referencia	S	S	S	S	S	S	S	S	S	S
Administrador	Traslado Entre Cuentas Bancarias	S	S	S	S	S	S	S	S	S	S
Administrador	Usuarios	S	S					S			
Administrador	Validación de Interés	S	S	S	S	S	S	S	S	S	S
Administrador Base de Datos	Limpieza Caché	S									
Administrador Usuarios	Roles	S	S		S			S			
Administrador Usuarios	Sesiones Activas				S			S			
Administrador Usuarios	Usuarios	S	S					S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Analista póliza localizados	Póliza Contrato Concesión	S		S	S		S	S	S	S	S
Analista póliza localizados	Reporte Contrato Concesión	S	S	S	S	S	S	S	S	S	S
Analista póliza localizados	Reporte Inventario Contrato Concesión	S	S	S	S	S	S	S	S	S	S
Analista póliza localizados	Reportes gestión contractual							S			
Aprobador póliza localizados	Gestión Contractual							S			
Aprobador póliza localizados	Póliza Contrato Concesión					S					
Aprobador póliza localizados	Reporte Contrato Concesión	S	S	S	S	S	S	S	S	S	S
Aprobador póliza localizados	Reporte inventario Contrato Concesión	S	S	S	S	S	S	S	S	S	S
Aprobador póliza localizados	Reportes gestión contractual							S			
Área Solicitante CAD I	Adendas términos de referencia	S	S		S			S			S
Área Solicitante CAD I	Contratación Administrativa							S			
Área Solicitante CAD I	Estudio Previo	S	S		S			S			
Área Solicitante CAD I	Solicitud Estudio de Mercado	S	S		S			S			
Área Solicitante CAD I	Términos de referencia	S	S		S			S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Cartera	Administración de Recursos Financieros							S			
Área Usuario cartera	Cartera							S			
Área Usuario Cartera	Contabilidad							S			
Área Usuario Cartera	Estado de cuenta Acuerdos de Pago	S	S	S	S	S	S	S	S	S	S
Área Usuario Cartera	Estado de cuenta GCT	S	S	S	S	S	S	S	S	S	S
Área Usuario Cartera	Estado de cuenta GENERAL	S	S	S	S	S	S	S	S	S	S
Área Usuario Cartera	Gestión Contractual							S			
Área Usuario Cartera	Parámetros							S			
Área Usuario Cartera	Recaudo y Transferencia							S			
Área Usuario Cartera	Reporte conciliación Contabilidad – Cartera	S	S	S	S	S	S	S	S	S	S
Área Usuario Cartera	Reportes Contabilidad							S			
Área Usuario Cartera	Tasas interés Súper financiera	S	S	S	S	S	S	S	S	S	S
Área Usuario Contratación Adm	Acta de Inicio	S	S	S	S	S	S	S	S	S	S
Área Usuario Contratación Adm	Adendas términos de referencia	S	S	S	S	S	S	S	S		S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Contratación Adm	Administración	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Administración de Recursos Financieros	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Alcance invitación proceso selección	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Contabilidad	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Contratación Administrativa	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Desarrollo de Mercados	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Designación supervisor	S	S	S	S	S	S	S	S	S	S
Área Usuario Contratación Adm	Estudio de Mercado	S	S	S	S	S	S	S	S	S	S
Área Usuario Contratación Adm	Estudio Previo	S	S	S	S	S	S	S	S	S	S
Área Usuario Contratación Adm	Evaluación de Propuestas	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Fuentes de Financiación	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Generación de la Minuta	S	S	S	S	S	S	S	S	S	S
Área Usuario Contratación Adm	Gestión Contractual	S	S	S	S	S	S	S	S		S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Contratación Adm	Modificación CDP	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Modificación RP	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	PAC y Tesorería	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Póliza Garantía	S	S	S	S	S	S	S	S	S	S
Área Usuario Contratación Adm	Presupuesto	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Proveedores	S	S	S	S	S	S	S	S	S	
Área Usuario Contratación Adm	Recaudo y Transferencia	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Recepción de Propuestas	S	S	S	S	S	S	S	S		S
Área Usuario Contratación Adm	Reportes Contabilidad							S			
Área Usuario Contratación Adm	Solicitud Estudio de Mercado	S	S	S	S	S	S	S	S	S	S
Área Usuario Contratación Adm	Términos de referencia	S	S	S	S	S	S	S	S		S
Área Usuario DME - GNA	Administración							S			
Área Usuario DME - GNA	Desarrollo de Mercados							S			
Área Usuario DME – GNA	Gestión Contractual							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario DME - GNA	Registro empresas	S	S	S	S	S	S	S	S	S	S
Área Usuario DME - GNN	Desarrollo de Mercados							S			
Área Usuario DME - GNN	Registro empresas							S			
Área Usuario GCT	Contratación Administrativa							S			
Área Usuario GCT	Estado de cuenta GCT	S	S	S	S	S	S	S	S	S	S
Área Usuario GCT	Estado de cuenta GENERAL	S	S	S	S	S	S	S	S	S	S
Área Usuario GCT	Estudio Previo	S	S	S	S	S	S	S	S	S	S
Área Usuario GCT	Gestión Contractual							S			
Área Usuario GCT	Marcación inventario no reportado	S	S	S	S	S	S	S	S	S	S
Área Usuario GCT	Recaudo y Transferencia							S			
Área Usuario GCT	Solicitud Estudio de Mercado	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Administración							S			
Área Usuario Gestión Contable	Administración de Recursos Financieros							S			
Área Usuario Gestión Contable	Balance de Prueba	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Carga de Contratos	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Cargar Nómina Funcionarios Planta	S	S	S	S	S	S	S	S	S	S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Gestión Contable	Centros de Costos	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Cierre Anual Contable	S				S					S
Área Usuario Gestión Contable	Cierre Mensual	S				S					S
Área Usuario Gestión Contable	Cierre recaudo	S				S		S			S
Área Usuario Gestión Contable	Conceptos Nómina	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Contabilidad							S			
Área Usuario Gestión Contable	Cuenta Contable	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Cuentas por pagar							S			
Área Usuario Gestión Contable	Cuentas por Tipo de Movimiento	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Estado de cuenta GCT	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Generar Obligación Transferencia ET	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Gestión Contractual							S			
Área Usuario Gestión Contable	Libro Auxiliar Por Comprobante	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Libro Auxiliar Por Rango de Cuentas	S	S	S	S	S	S	S	S	S	S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Gestión Contable	Nómina							S			
Área Usuario Gestión Contable	Obligación	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Obligación Funcionarios Planta	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Obligación No presupuestal	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Obligación Transferencia ET	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Parámetros							S			
Área Usuario Gestión Contable	Presupuesto							S			
Área Usuario Gestión Contable	Procesamiento Contabilidad							S			
Área Usuario Gestión Contable	Procesamiento cuentas por pagar							S			
Área Usuario Gestión Contable	Procesamiento Nómina							S			
Área Usuario Gestión Contable	Proveedores	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Recaudo y Transferencia							S			
Área Usuario Gestión Contable	Registro Comprobante Contable	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Reporte Conciliación Contabilidad - Cartera	S	S	S	S	S	S	S	S		S
Área Usuario Gestión Contable	Reportes Contabilidad							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Gestión Contable	Tipo Comprobante Contable	S	S	S	S	S	S	S	S	S	S
Área Usuario Gestión Contable	Tipo Retención	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Adición Presupuestal	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Administración	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Administración de Recursos Financieros	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	CDP Expedidos	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Contabilidad	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Contratación Administrativa	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Decremento CDP	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Decremento RP	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Desarrollo de Mercados	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Estudio Previo	S	S	S	S			S			
Área Usuario Presupuesto	Expedición CDP	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Expedir RP masivo nómina	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Fuentes de Financiación	S	S	S	S	S	S	S	S		S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Presupuesto	Gestión Contractual	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Incremento CDP	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Incremento de RP	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Modificación CDP	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Modificación RP	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	PAC y Tesorería	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Pagos Ejecutados 4xMil				S			S			S
Área Usuario Presupuesto	Presupuesto	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Recaudo y Transferencia	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Reducción Presupuestal	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Registrar Programación PFC mensual	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Registro Apropriación Inicial	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Registro Presupuestal	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Registro Traslado Presupuestal	S	S	S	S	S	S	S	S	S	S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Presupuesto	Reporte Auxiliar por Terceros				S			S			S
Área Usuario Presupuesto	Reporte Cadena Presupuestal	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Reporte Ejecución presupuestal de gastos	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Reporte Ejecución presupuestal de ingresos	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Reportes Modificación CDP	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Reportes Modificación RP	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Reportes Presupuesto							S			
Área Usuario Presupuesto	RP Expedidos	S	S	S	S	S	S	S	S	S	S
Área Usuario Presupuesto	Solicitud CDP	S	S	S	S	S	S	S	S		S
Área Usuario Presupuesto	Solicitud Estudio de Mercado	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Administración	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Administración de Recursos Financieros	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Cargue Documento CONPES	S				S	S	S			
Área Usuario Tesorería	Cierre recaudo	S	S					S			
$A = \pi r^2$ 36 Usuario Tesorería	Contabilidad	S	S	S	S	S	S	S	S		S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Tesorería	Contratación Administrativa	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Desarrollo de Mercados	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Distribución	S			S	S	S	S			S
Área Usuario Tesorería	Fuentes de Financiación	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Generar Orden de Pago Transferencia ET	S			S	S		S			S
Área Usuario Tesorería	Gestión Contractual	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Modificación CDP	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Modificación RP	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Orden de Pago	S	S	S	S	S	S	S	S	S	S
Área Usuario Tesorería	Orden de Pago Cuentas por Pagar	S	S	S	S	S	S	S	S	S	S
Área Usuario Tesorería	Orden de Pago Funcionarios Planta	S	S	S	S	S	S	S	S	S	S
Área Usuario Tesorería	Orden de pago No presupuestal	S	S	S	S	S	S	S	S	S	S
Área Usuario Tesorería	Orden de Pago Nómina Funcionarios Planta	S	S	S	S	S	S	S	S	S	S
Área Usuario Tesorería	Orden de Pago Transferencia ET	S	S		S	S		S			S
Área Usuario Tesorería	PAC y Tesorería	S	S	S	S	S	S	S	S		S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Área Usuario Tesorería	Pago Operadores en Banco	S	S	S	S	S	S	S	S	S	S
Área Usuario Tesorería	Presupuesto	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Proyección Flujo de Caja	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Recaudo y Transferencia	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Registrar Programación PFC mensual	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Registro Aprobación PAC mensual	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Registro Solicitud PFC mensual	S	S	S	S	S	S	S	S		S
Área Usuario Tesorería	Saldo Inicial Cuentas Bancarias	S	S	S	S	S	S	S	S	S	S
Área Usuario Tesorería	Solicitud de Pago	S	S	S	S	S	S	S	S	S	S
Área Usuario Tesorería	Traslado Entre Cuentas Bancarias	S	S	S	S	S	S	S	S	S	S
AUDITORIAS ENTES DE CONTROL	Acta de Inicio							S			
AUDITORIAS ENTES DE CONTROL	Acuerdos de pago							S			
AUDITORIAS ENTES DE CONTROL	Adendas términos de referencia							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
AUDITORIAS ENTES DE CONTROL	Adjudicación							S			
AUDITORIAS ENTES DE CONTROL	Administración							S			
AUDITORIAS ENTES DE CONTROL	Administración de Recursos Financieros							S			
AUDITORIAS ENTES DE CONTROL	Alcance invitación proceso selección							S			
AUDITORIAS ENTES DE CONTROL	Balance de Prueba							S			
AUDITORIAS ENTES DE CONTROL	Beneficiarios ET							S			
AUDITORIAS ENTES DE CONTROL	Carga de Contratos							S			
AUDITORIAS ENTES DE CONTROL	Cargar Nómina Funcionarios Planta							S			
AUDITORIAS ENTES DE CONTROL	Cargue Documento CONPES							S			
AUDITORIAS ENTES DE CONTROL	CDP Expedidos							S			
AUDITORIAS ENTES DE CONTROL	Cierre Mensual							S			
AUDITORIAS ENTES DE CONTROL	Cierre recaudo							S			
AUDITORIAS ENTES DE CONTROL	Contabilidad							S			
AUDITORIAS ENTES DE CONTROL	Contratación Administrativa							S			
AUDITORIAS ENTES DE CONTROL	Contrato de Concesión							S			
AUDITORIAS ENTES DE CONTROL	Cuenta Contable							S			
AUDITORIAS ENTES DE CONTROL	Cuentas por pagar							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
AUDITORIAS ENTES DE CONTROL	Decremento RP							S			
AUDITORIAS ENTES DE CONTROL	Desarrollo de Mercados							S			
AUDITORIAS ENTES DE CONTROL	Designación supervisor							S			
AUDITORIAS ENTES DE CONTROL	Distribución							S			
AUDITORIAS ENTES DE CONTROL	Estado de cuenta Acuerdos de Pago							S			
AUDITORIAS ENTES DE CONTROL	Estado de cuenta GCT							S			
AUDITORIAS ENTES DE CONTROL	Estado de cuenta GENERAL				S			S			S
AUDITORIAS ENTES DE CONTROL	Estudio de Mercado							S			
AUDITORIAS ENTES DE CONTROL	Estudio Previo							S			
AUDITORIAS ENTES DE CONTROL	Evaluación de Propuestas							S			
AUDITORIAS ENTES DE CONTROL	Expedición CDP							S			
AUDITORIAS ENTES DE CONTROL	Expedir RP masivo nómina							S			
AUDITORIAS ENTES DE CONTROL	Generación de la Minuta							S			
AUDITORIAS ENTES DE CONTROL	Generar Obligación Transferencia ET							S			
AUDITORIAS ENTES DE CONTROL	Generar Orden de Pago Transferencia ET							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
AUDITORIAS ENTES DE CONTROL	Incremento CDP							S			
AUDITORIAS ENTES DE CONTROL	Incremento de RP							S			
AUDITORIAS ENTES DE CONTROL	Invitación proceso de selección							S			
AUDITORIAS ENTES DE CONTROL	Libro Auxiliar Por Comprobante							S			
AUDITORIAS ENTES DE CONTROL	Libro Auxiliar Por Rango de Cuentas							S			
AUDITORIAS ENTES DE CONTROL	Liquidación contrato concesión							S			
AUDITORIAS ENTES DE CONTROL	Liquidación Mensual							S			
AUDITORIAS ENTES DE CONTROL	Marcación inventario no reportado							S			
AUDITORIAS ENTES DE CONTROL	Modificación CDP							S			
AUDITORIAS ENTES DE CONTROL	Modificación RP							S			
AUDITORIAS ENTES DE CONTROL	Nómina							S			
AUDITORIAS ENTES DE CONTROL	Obligación							S			
AUDITORIAS ENTES DE CONTROL	Obligación Funcionarios Planta							S			
AUDITORIAS ENTES DE CONTROL	Obligación No presupuestal							S			
AUDITORIAS ENTES DE CONTROL	Obligación Transferencia ET							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
AUDITORIAS ENTES DE CONTROL	Oficio de Liquidación							S			
AUDITORIAS ENTES DE CONTROL	Oficio de Liquidación Contrato Nuevo							S			
AUDITORIAS ENTES DE CONTROL	Oficio de Liquidación Modificación Contrato							S			
AUDITORIAS ENTES DE CONTROL	Orden de Pago							S			
AUDITORIAS ENTES DE CONTROL	Orden de Pago Cuentas por Pagar							S			
AUDITORIAS ENTES DE CONTROL	Orden de Pago Funcionarios Planta							S			
AUDITORIAS ENTES DE CONTROL	Orden de Pago Nómina Funcionarios Planta							S			
AUDITORIAS ENTES DE CONTROL	Orden de Pago Transferencia ET							S			
AUDITORIAS ENTES DE CONTROL	Otrosí Contrato de Concesión							S			
AUDITORIAS ENTES DE CONTROL	PAC y Tesorería							S			
AUDITORIAS ENTES DE CONTROL	Pago Operadores en Banco				S			S			S
AUDITORIAS ENTES DE CONTROL	Pagos Ejecutados 4xMil							S			
AUDITORIAS ENTES DE CONTROL	Parámetros							S			
AUDITORIAS ENTES DE CONTROL	Póliza Contrato Concesión							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
AUDITORIAS ENTES DE CONTROL	Póliza Otrosi Contrato de Concesión							S			
AUDITORIAS ENTES DE CONTROL	Presupuesto							S			
AUDITORIAS ENTES DE CONTROL	Procesamiento Contabilidad							S			
AUDITORIAS ENTES DE CONTROL	Procesamiento cuentas por pagar							S			
AUDITORIAS ENTES DE CONTROL	Procesamiento Nómina							S			
AUDITORIAS ENTES DE CONTROL	Proveedores							S			
AUDITORIAS ENTES DE CONTROL	Proyección Flujo de Caja							S			
AUDITORIAS ENTES DE CONTROL	Recaudo y Transferencia							S			
AUDITORIAS ENTES DE CONTROL	Recepción de Propuestas							S			
AUDITORIAS ENTES DE CONTROL	Reducción Presupuestal							S			
AUDITORIAS ENTES DE CONTROL	Registrar Programación PFC mensual							S			
AUDITORIAS ENTES DE CONTROL	Registro Aprobación PAC mensual							S			
AUDITORIAS ENTES DE CONTROL	Registro Apropriación Inicial							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
AUDITORIAS ENTES DE CONTROL	Registro de Aprobación PAC							S			
AUDITORIAS ENTES DE CONTROL	Registro empresas							S			
AUDITORIAS ENTES DE CONTROL	Registro Presupuestal							S			
AUDITORIAS ENTES DE CONTROL	Registro Solicitud PFC mensual							S			
AUDITORIAS ENTES DE CONTROL	Registro Traslado Presupuestal							S			
AUDITORIAS ENTES DE CONTROL	Renovación Póliza Contrato de Concesión							S			
AUDITORIAS ENTES DE CONTROL	Reporte Cadena Presupuestal							S			
AUDITORIAS ENTES DE CONTROL	Reporte Conciliación Contabilidad - Cartera							S			
AUDITORIAS ENTES DE CONTROL	Reporte Contrato Concesión							S			
AUDITORIAS ENTES DE CONTROL	Reporte Ejecución presupuestal de gastos							S			
AUDITORIAS ENTES DE CONTROL	Reporte Ejecución presupuestal de ingresos							S			
AUDITORIAS ENTES DE CONTROL	Reporte Inventario Contrato Concesión							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
AUDITORIAS ENTES DE CONTROL	Reportes Contabilidad							S			
AUDITORIAS ENTES DE CONTROL	Reportes gestión contractual							S			
AUDITORIAS ENTES DE CONTROL	Reportes Liquidación Mensual							S			
AUDITORIAS ENTES DE CONTROL	Reportes Modificación CDP							S			
AUDITORIAS ENTES DE CONTROL	Reportes Modificación RP							S			
AUDITORIAS ENTES DE CONTROL	Reportes Presupuesto							S			
AUDITORIAS ENTES DE CONTROL	Resolución Autorización Localizados							S			
AUDITORIAS ENTES DE CONTROL	Roles							S			
AUDITORIAS ENTES DE CONTROL	RP Expedidos							S			
AUDITORIAS ENTES DE CONTROL	Saldo Inicial Cuentas Bancarias							S			
AUDITORIAS ENTES DE CONTROL	Sesiones Activas							S			
AUDITORIAS ENTES DE CONTROL	Solicitud autorización de rifas							S			
AUDITORIAS ENTES DE CONTROL	Solicitud autorización promocionales							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
AUDITORIAS ENTES DE CONTROL	Solicitud de Pago							S			
AUDITORIAS ENTES DE CONTROL	Solicitud Estudio de Mercado							S			
AUDITORIAS ENTES DE CONTROL	Tasas interés Súper financiera							S			
AUDITORIAS ENTES DE CONTROL	Términos de referencia							S			
AUDITORIAS ENTES DE CONTROL	Tipo Comprobante Contable							S			
AUDITORIAS ENTES DE CONTROL	Tipo Retención							S			
AUDITORIAS ENTES DE CONTROL	Traslado Entre Cuentas Bancarias							S			
AUDITORIAS ENTES DE CONTROL	Traslado entre ítems del Plan de contratación							S			
AUDITORIAS ENTES DE CONTROL	Usuarios							S			
AUDITORIAS ENTES DE CONTROL	Validación de Interés							S			
Auxiliar CAD I	Adendas términos de referencia	S	S		S			S			S
Auxiliar CAD I	Adjudicación	S	S	S	S			S			S
Auxiliar CAD I	Administración de Recursos Financieros							S			
Auxiliar CAD I	Contabilidad							S			
Auxiliar CAD I	Contratación Administrativa							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Auxiliar CAD I	Estudio de Mercado	S	S	S	S	S	S	S	S	S	S
Auxiliar CAD I	Estudio Previo	S	S	S	S	S	S	S	S	S	S
Auxiliar CAD I	Evaluación de Propuestas	S	S	S	S	S		S			S
Auxiliar CAD I	Generación de la Minuta	S	S	S	S	S		S			S
Auxiliar CAD I	Invitación proceso de selección	S	S	S	S	S	S	S	S	S	S
Auxiliar CAD I	Póliza Garantía	S	S	S	S	S		S			S
Auxiliar CAD I	Proveedores	S	S	S	S			S			
Auxiliar CAD I	Recepción de Propuestas	S	S	S	S	S		S			S
Auxiliar CAD I	Solicitud Estudio de Mercado	S	S	S	S	S	S	S	S	S	S
Auxiliar CAD I	Términos de referencia	S	S	S	S			S			S
Auxiliar Cartera GCT	Estado de cuenta GCT	S	S	S	S	S	S	S	S	S	S
Auxiliar Cartera GCT	Estado de cuenta GENERAL	S	S	S	S	S	S	S	S	S	S
Auxiliar Cartera GCT	Gestión Contractual							S			
Auxiliar Cartera GCT	Recaudo y Transferencia							S			
Auxiliar Contable SENA	Administración de Recursos Financieros							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Auxiliar Contable SENA	Proveedores	S	S		S			S		S	S
Auxiliar Contable SENA	Reportes Contabilidad							S			
Auxiliar DME GNN	Desarrollo de Mercados							S			
Auxiliar DME GNN	Registro empresas	S						S			
Auxiliar GCT Marcador	Gestión Contractual							S			
Auxiliar GCT Marcador	Marcación inventario no reportado	S	S	S	S	S	S	S	S	S	S
Auxiliar Gestión Contable I	Administración de Recursos Financieros							S			
Auxiliar Gestión Contable I	Balance de Prueba	S	S	S	S			S		S	S
Auxiliar Gestión Contable I	Cargar Nómina Funcionarios Planta	S	S	S	S			S		S	S
Auxiliar Gestión Contable I	Cargue Masivo Comprobantes Contables	S	S	S	S	S	S	S	S	S	S
Auxiliar Gestión Contable I	Contabilidad							S			
Auxiliar Gestión Contable I	Cuentas por pagar							S			
Auxiliar Gestión Contable I	Estado de cuenta GENERAL	S	S	S	S	S	S	S	S	S	S
Auxiliar Gestión Contable I	Libro Auxiliar Por Comprobante	S	S	S	S			S			S
Auxiliar Gestión Contable I	Libro Auxiliar Por Rango de Cuentas	S	S	S	S			S			S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Auxiliar Gestión Contable I	Nómina							S			
Auxiliar Gestión Contable I	Obligación	S	S	S	S			S			S
Auxiliar Gestión Contable I	Obligación Funcionarios Planta	S	S	S	S			S			S
Auxiliar Gestión Contable I	Obligación No presupuestal	S	S	S	S			S			S
Auxiliar Gestión Contable I	Procesamiento Contabilidad							S			
Auxiliar Gestión Contable I	Procesamiento cuentas por pagar							S			
Auxiliar Gestión Contable I	Procesamiento Nómina							S			
Auxiliar Gestión Contable I	Recaudo y Transferencia							S			
Auxiliar Gestión Contable I	Registro Comprobante Contable	S	S	S	S			S			S
Auxiliar Gestión Contable I	Reportes Contabilidad							S			
Auxiliar Gestión Contable II	Administración de Recursos Financieros							S			
Auxiliar Gestión Contable II	Balance de Prueba							S			
Auxiliar Gestión Contable II	Contabilidad							S			
Auxiliar Gestión Contable II	Cuentas por pagar							S			
Auxiliar Gestión Contable II	Libro Auxiliar Por Comprobante				S			S			S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Auxiliar Gestión Contable II	Obligación Funcionarios Planta							S			
Auxiliar Gestión Contable II	Obligación No presupuestal							S			
Auxiliar Gestión Contable II	Procesamiento Contabilidad							S			
Auxiliar Gestión Contable II	Procesamiento cuentas por pagar							S			
Auxiliar Gestión Contable II	Registro Comprobante Contable							S			
Auxiliar Gestión Contable II	Reportes Contabilidad							S			
Auxiliar Gestión Contable III	Administración de Recursos Financieros							S			
Auxiliar Gestión Contable III	Balance de Prueba	S	S	S	S			S			S
Auxiliar Gestión Contable III	Cargue Masivo Comprobantes Contables	S	S	S	S	S	S	S	S	S	S
Auxiliar Gestión Contable III	Contabilidad							S			
Auxiliar Gestión Contable III	Cuentas por pagar							S			
Auxiliar Gestión Contable III	Estado de cuenta GCT	S	S	S	S	S	S	S	S	S	S
Auxiliar Gestión Contable III	Gestión Contractual							S			
Auxiliar Gestión Contable III	Libro Auxiliar Por Comprobante	S	S	S	S			S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Auxiliar Gestión Contable III	Obligación	S	S	S				S			
Auxiliar Gestión Contable III	Obligación Funcionarios Planta	S	S	S				S			
Auxiliar Gestión Contable III	Procesamiento Contabilidad							S			
Auxiliar Gestión Contable III	Procesamiento cuentas por pagar							S			
Auxiliar Gestión Contable III	Registro Comprobante Contable	S	S	S				S			
Auxiliar Gestión Contable III	Reportes Contabilidad							S			
Auxiliar Tesorería	Administración de Recursos Financieros							S			
Auxiliar Tesorería	Cargue Documento CONPES	S	S	S	S	S	S	S	S	S	S
Auxiliar Tesorería	PAC y Tesorería							S			
Auxiliar Tesorería	Pago Operadores en Banco	S	S	S	S		S	S	S	S	S
Auxiliar Tesorería	Recaudo y Transferencia							S			
Auxiliar Tesorería	Solicitud de Pago	S	S	S	S	S	S	S	S	S	S
CN Abogado revisor	Contrato de Concesión	S	S		S		S				

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
CN Abogado revisor	Resolución Autorización Localizados		S		S		S				
CN Administrador	Contrato de Concesión				S			S			
CN Administrador	Desarrollo de Mercados							S			
CN Administrador	Gestión Contractual							S			
CN Administrador	Oficio de Liquidación							S			
CN Administrador	Oficio de Liquidación Contrato Nuevo				S			S			
CN Administrador	Póliza Contrato Concesión				S			S			
CN Administrador	Resolución Autorización Localizados				S			S			
CN Analista GNA	Desarrollo de Mercados							S			
CN Analista GNA	Gestión Contractual							S			
CN Analista GNA	Oficio de Liquidación							S			
CN Analista GNA	Oficio de Liquidación Contrato Nuevo	S	S		S	S					
CN Analista GNA	Póliza Contrato Concesión	S	S		S	S			S		

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
CN Canal de distribución	Contrato de Concesión		S		S					S	
CN Canal de distribución	Desarrollo de Mercados							S			
CN Canal de distribución	Resolución Autorización Localizados		S		S					S	
CN Evaluador CCO	Contrato de Concesión		S		S						S
CN Evaluador CCO	Desarrollo de Mercados							S			
CN Evaluador financiero	Contrato de Concesión		S		S			S			
CN Evaluador financiero	Desarrollo de Mercados							S			
CN Evaluador financiero	Oficio de Liquidación							S			
CN Evaluador financiero	Oficio de Liquidación Contrato Nuevo				S					S	
CN Evaluador financiero	Resolución Autorización Localizados		S		S			S			
CN Evaluador GCT	Contrato de Concesión		S		S				S		
CN Evaluador GCT	Desarrollo de Mercados							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
CN Evaluador GCT	Resolución Autorización Localizados		S		S				S		
CN Notificaciones SAC	Contrato de Concesión		S	S	S						
CN Notificaciones SAC	Desarrollo de Mercados							S			
CN Notificaciones SAC	Resolución Autorización Localizados		S	S	S						
CONSULTA SEGURIDAD Y CALIDAD	Administración							S			
CONSULTA SEGURIDAD Y CALIDAD	Roles							S			
CONSULTA SEGURIDAD Y CALIDAD	Sesiones Activas							S			
CONSULTA SEGURIDAD Y CALIDAD	Usuarios							S			
Consultas / Soporte usuario	Acta de Inicio							S			
Consultas / Soporte usuario	Acuerdos de pago							S			
Consultas / Soporte usuario	Adendas términos de referencia							S			
Consultas / Soporte usuario	Adición Presupuestal							S			
Consultas / Soporte usuario	Adjudicación							S			
Consultas / Soporte usuario	Administración							S			
Consultas / Soporte usuario	Administración de Recursos Financieros							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Consultas / Soporte usuario	Alcance invitación proceso selección							S			
Consultas / Soporte usuario	Balance de Prueba							S			
Consultas / Soporte usuario	Cargar Nómina Funcionarios Planta							S			
Consultas / Soporte usuario	Cargue Documento CONPES							S			
Consultas / Soporte usuario	Cartera							S			
Consultas / Soporte usuario	CDP Expedidos							S			
Consultas / Soporte usuario	Cierre Mensual							S			
Consultas / Soporte usuario	Cierre recaudo							S			
Consultas / Soporte usuario	Contabilidad							S			
Consultas / Soporte usuario	Contratación Administrativa							S			
Consultas / Soporte usuario	Contrato de Concesión							S			
Consultas / Soporte usuario	Cuentas por pagar							S			
Consultas / Soporte usuario	Decremento CDP							S			
Consultas / Soporte usuario	Decremento RP							S			
Consultas / Soporte usuario	Desarrollo de Mercados							S			
Consultas / Soporte usuario	Designación supervisor							S			
Consultas / Soporte usuario	Distribución							S			
Consultas / Soporte usuario	Estado de cuenta Acuerdos de Pago							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Consultas / Soporte usuario	Estado de cuenta GCT							S			
Consultas / Soporte usuario	Estado de cuenta GENERAL							S			
Consultas / Soporte usuario	Estudio de Mercado							S			
Consultas / Soporte usuario	Estudio Previo							S			
Consultas / Soporte usuario	Evaluación de Propuestas							S			
Consultas / Soporte usuario	Expedición CDP							S			
Consultas / Soporte usuario	Expedir RP masivo nómina							S			
Consultas / Soporte usuario	Generación de la Minuta							S			
Consultas / Soporte usuario	Generar Obligación Transferencia ET							S			
Consultas / Soporte usuario	Generar Orden de Pago Transferencia ET							S			
Consultas / Soporte usuario	Gestión Contractual							S			
Consultas / Soporte usuario	Incremento CDP							S			
Consultas / Soporte usuario	Incremento de RP							S			
Consultas / Soporte usuario	Invitación proceso de selección							S			
Consultas / Soporte usuario	Libro Auxiliar Por Comprobante							S			
Consultas / Soporte usuario	Libro Auxiliar Por Rango de Cuentas							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Consultas / Soporte usuario	Liquidación Mensual							S			
Consultas / Soporte usuario	Modificación CDP							S			
Consultas / Soporte usuario	Modificación RP							S			
Consultas / Soporte usuario	Nómina							S			
Consultas / Soporte usuario	Obligación							S			
Consultas / Soporte usuario	Obligación Funcionarios Planta							S			
Consultas / Soporte usuario	Obligación No presupuestal							S			
Consultas / Soporte usuario	Obligación Transferencia ET							S			
Consultas / Soporte usuario	Oficio de Liquidación							S			
Consultas / Soporte usuario	Oficio de Liquidación Contrato Nuevo							S			
Consultas / Soporte usuario	Oficio de Liquidación Modificación Contrato							S			
Consultas / Soporte usuario	Orden de Pago							S			
Consultas / Soporte usuario	Orden de Pago Cuentas por Pagar							S			
Consultas / Soporte usuario	Orden de Pago Funcionarios Planta							S			
Consultas / Soporte usuario	Orden de pago No presupuestal							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Consultas / Soporte usuario	Orden de Pago Nómina Funcionarios Planta							S			
Consultas / Soporte usuario	Orden de Pago Transferencia ET							S			
Consultas / Soporte usuario	PAC y Tesorería							S			
Consultas / Soporte usuario	Pago Operadores en Banco							S			
Consultas / Soporte usuario	Parámetros							S			
Consultas / Soporte usuario	Póliza Contrato Concesión							S			
Consultas / Soporte usuario	Póliza Garantía							S			
Consultas / Soporte usuario	Presupuesto							S			
Consultas / Soporte usuario	Procesamiento Contabilidad							S			
Consultas / Soporte usuario	Procesamiento cuentas por pagar							S			
Consultas / Soporte usuario	Procesamiento Nómina							S			
Consultas / Soporte usuario	Proveedores							S			
Consultas / Soporte usuario	Proyección Flujo de Caja							S			
Consultas / Soporte usuario	Recaudo y Transferencia							S			
Consultas / Soporte usuario	Recepción de Propuestas							S			
Consultas / Soporte usuario	Reducción Presupuestal							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Consultas / Soporte usuario	Registrar Programación PFC mensual							S			
Consultas / Soporte usuario	Registro Aprobación PAC mensual							S			
Consultas / Soporte usuario	Registro Apropiación Inicial							S			
Consultas / Soporte usuario	Registro Comprobante Contable							S			
Consultas / Soporte usuario	Registro de Aprobación PAC							S			
Consultas / Soporte usuario	Registro empresas							S			
Consultas / Soporte usuario	Registro Presupuestal							S			
Consultas / Soporte usuario	Registro Solicitud PFC mensual							S			
Consultas / Soporte usuario	Registro Traslado Presupuestal							S			
Consultas / Soporte usuario	Reporte Cadena Presupuestal							S			
Consultas / Soporte usuario	Reporte Conciliación Contabilidad – Cartera							S			
Consultas / Soporte usuario	Reporte Ejecución presupuestal de gastos							S			
Consultas / Soporte usuario	Reporte Ejecución presupuestal de ingresos							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Consultas / Soporte usuario	Reporte Inventario Contrato Concesión							S			
Consultas / Soporte usuario	Reporte Liquidación mensual							S			
Consultas / Soporte usuario	Reportes Contabilidad							S			
Consultas / Soporte usuario	Reportes gestión contractual							S			
Consultas / Soporte usuario	Reportes Liquidación Mensual							S			
Consultas / Soporte usuario	Reportes Modificación CDP							S			
Consultas / Soporte usuario	Reportes Modificación RP							S			
Consultas / Soporte usuario	Reportes Presupuesto							S			
Consultas / Soporte usuario	Resolución Autorización Localizados							S			
Consultas / Soporte usuario	Roles							S			
Consultas / Soporte usuario	RP Expedidos							S			
Consultas / Soporte usuario	Saldo Inicial Cuentas Bancarias							S			
Consultas / Soporte usuario	Sesiones Activas							S			
Consultas / Soporte usuario	Solicitud CDP							S			
Consultas / Soporte usuario	Solicitud de Pago							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Consultas / Soporte usuario	Solicitud Estudio de Mercado							S			
Consultas / Soporte usuario	Tasas interés Súper financiera							S			
Consultas / Soporte usuario	Términos de referencia							S			
Consultas / Soporte usuario	Traslado Entre Cuentas Bancarias							S			
Consultas / Soporte usuario	Usuarios							S			
Consultas / Soporte usuario	Validación de Interés							S			
Control Interno	Administración							S			
Control Interno	Administración de Recursos Financieros							S			
Control Interno	Balance de Prueba				S			S			S
Control Interno	Cartera							S			
Control Interno	Contabilidad							S			
Control Interno	Contratación Administrativa							S			
Control Interno	Cuentas por pagar							S			
Control Interno	Desarrollo de Mercados							S			
Control Interno	Gestión Contractual							S			
Control Interno	Libro Auxiliar Por Comprobante				S			S			S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Control Interno	Libro Auxiliar Por Rango de Cuentas				S			S			S
Control Interno	Liquidación Mensual							S			
Control Interno	Modificación CDP							S			
Control Interno	Modificación RP							S			
Control Interno	Nómina							S			
Control Interno	Oficio de Liquidación							S			
Control Interno	PAC y Tesorería							S			
Control Interno	Presupuesto							S			
Control Interno	Procesamiento Contabilidad							S			
Control Interno	Procesamiento cuentas por pagar							S			
Control Interno	Procesamiento Nómina							S			
Control Interno	Recaudo y Transferencia							S			
Control Interno	Reporte Conciliación Contabilidad - Cartera							S			
Control Interno	Reporte Ejecución presupuestal de gastos							S			
Control Interno	Reporte Liquidación mensual							S			
Control Interno	Reportes Contabilidad							S			
Control Interno	Reportes Liquidación Mensual							S			
Control Interno	Reportes Presupuesto							S			
Ejecutor Manual Procesos Cartera	Administración							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Ejecutor Manual Procesos Cartera	Interés Diario	S									
Ejecutor Manual Procesos Cartera	Pago Operadores PSE	S									
Jefe Área Solicitante CAD	Adendas términos de referencia	S	S	S	S	S	S	S	S	S	S
Jefe Área Solicitante CAD	Contratación Administrativa							S			
Jefe Área Solicitante CAD	Estudio Previo	S	S		S	S		S			S
Jefe Área Solicitante CAD	Solicitud Estudio de Mercado	S	S	S	S	S		S	S		S
Jefe Área Solicitante CAD	Términos de referencia	S	S	S	S	S		S	S		S
Jefes Consultas	Acta de Inicio							S			
Jefes Consultas	Adendas términos de referencia							S			
Jefes Consultas	Adición Presupuestal							S			
Jefes Consultas	Administración de Recursos Financieros							S			
Jefes Consultas	Cargar Nómina Funcionarios Planta							S			
Jefes Consultas	Cargue Documento CONPES							S			
Jefes Consultas	Cierre Mensual							S			
Jefes Consultas	Cierre recaudo							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Jefes Consultas	Contabilidad							S			
Jefes Consultas	Contratación Administrativa							S			
Jefes Consultas	Contrato de Concesión							S			
Jefes Consultas	Decremento CDP							S			
Jefes Consultas	Decremento RP							S			
Jefes Consultas	Desarrollo de Mercados							S			
Jefes Consultas	Designación supervisor							S			
Jefes Consultas	Estado de cuenta Acuerdos de Pago							S			
Jefes Consultas	Estado de cuenta GENERAL							S			
Jefes Consultas	Estudio de Mercado							S			
Jefes Consultas	Estudio Previo							S			
Jefes Consultas	Evaluación de Propuestas							S			
Jefes Consultas	Expedición CDP							S			
Jefes Consultas	Generación de la Minuta							S			
Jefes Consultas	Gestión Contractual							S			
Jefes Consultas	Incremento CDP							S			
Jefes Consultas	Invitación proceso de selección							S			
Jefes Consultas	Libro Auxiliar Por Comprobante							S			
Jefes Consultas	Libro Auxiliar Por Rango de Cuentas							S			
Jefes Consultas	Modificación CDP							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Jefes Consultas	Modificación RP							S			
Jefes Consultas	Obligación							S			
Jefes Consultas	Obligación No presupuestal							S			
Jefes Consultas	Oficio de Liquidación							S			
Jefes Consultas	Oficio de Liquidación Contrato Nuevo							S			
Jefes Consultas	Oficio de Liquidación Modificación Contrato							S			
Jefes Consultas	Orden de Pago							S			
Jefes Consultas	Orden de Pago Cuentas por Pagar							S			
Jefes Consultas	Orden de pago No presupuestal							S			
Jefes Consultas	PAC y Tesorería							S			
Jefes Consultas	Pago Operadores en Banco							S			
Jefes Consultas	Póliza Contrato Concesión							S			
Jefes Consultas	Póliza Garantía							S			
Jefes Consultas	Presupuesto							S			
Jefes Consultas	Proveedores							S			
Jefes Consultas	Proyección Flujo de Caja							S			
Jefes Consultas	Recaudo y Transferencia							S			
Jefes Consultas	Recepción de Propuestas							S			
Jefes Consultas	Reducción Presupuestal							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Jefes Consultas	Registrar Programación PFC mensual							S			
Jefes Consultas	Registro Aprobación PAC mensual							S			
Jefes Consultas	Registro Apropiación Inicial							S			
Jefes Consultas	Registro Comprobante Contable							S			
Jefes Consultas	Registro de Aprobación PAC							S			
Jefes Consultas	Registro empresas							S			
Jefes Consultas	Registro Presupuestal							S			
Jefes Consultas	Registro Solicitud PFC mensual							S			
Jefes Consultas	Registro Traslado Presupuestal							S			
Jefes Consultas	Reporte Ejecución presupuestal de gastos							S			
Jefes Consultas	Reportes Presupuesto							S			
Jefes Consultas	Resolución Autorización Localizados							S			
Jefes Consultas	Saldo Inicial Cuentas Bancarias							S			
Jefes Consultas	Sesiones Activas							S			
Jefes Consultas	Solicitud CDP							S			
Jefes Consultas	Solicitud de Pago							S			
Jefes Consultas	Solicitud Estudio de Mercado							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Jefes Consultas	Términos de referencia							S			
Jefes Consultas	Traslado Entre Cuentas Bancarias							S			
Jefes Consultas	Validación de Interés							S			
PR Administrador	Desarrollo de Mercados							S			
PR Administrador	Solicitud autorización promocionales				S			S			
PR Analista GNA	Desarrollo de Mercados							S			
PR Analista GNA	Solicitud autorización promocionales	S	S		S		S	S			
PR Notificaciones SAC	Desarrollo de Mercados							S			
PR Notificaciones SAC	Solicitud autorización promocionales					S			S		
Profesional Tesorería	Administración de Recursos Financieros							S			
Profesional Tesorería	Cargue Documento CONPES	S						S			
Profesional Tesorería	Distribución	S			S			S			
Profesional Tesorería	Generar Orden de Pago Transferencia ET	S			S			S			
Profesional Tesorería	Orden de Pago	S			S			S			S
Profesional Tesorería	Orden de Pago Cuentas por Pagar	S			S			S			S
Profesional Tesorería	Orden de Pago Funcionarios Planta	S			S			S			S
Profesional Tesorería	Orden de pago No presupuestal	S			S			S			S

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Profesional Tesorería	Orden de Pago Nómina Funcionarios Planta	S			S			S			S
Profesional Tesorería	Orden de Pago Transferencia ET	S	S		S			S			
Profesional Tesorería	PAC y Tesorería							S			
Profesional Tesorería	Recaudo y Transferencia							S			
Profesional Tesorería	Solicitud de Pago	S	S	S	S	S	S	S	S	S	S
Técnico II Tesorería	Administración de Recursos Financieros							S			
Técnico II Tesorería	Cargue Documento CONPES	S						S			
Técnico II Tesorería	Distribución	S			S			S			
Técnico II Tesorería	Generar Orden de Pago Transferencia ET	S			S			S			
Técnico II Tesorería	Orden de Pago Transferencia ET	S	S		S			S			
Técnico II Tesorería	PAC y Tesorería							S			
Técnico II Tesorería	Recaudo y Transferencia							S			
Usuario Verificación Cartera	Administración de Recursos Financieros							S			
Usuario Verificación Cartera	Contabilidad							S			
Usuario Verificación Cartera	Estado de cuenta Acuerdos de Pago	S	S	S	S	S	S	S	S	S	S
Usuario Verificación Cartera	Estado de cuenta GCT	S	S	S	S	S	S	S	S	S	S
Usuario Verificación Cartera	Estado de cuenta GENERAL	S	S	S	S	S	S	S	S	S	S
Usuario Verificación Cartera	Gestión Contractual							S			

Continuación Cuadro 10. Roles, módulos y permisos SIICOL.

Rol	Módulo	Registrar	Modificar	Borrar	Imprimir	Aprobar	Rechazar	Consultar	Devolver	Revisar	Generar
Usuario Verificación Cartera	Proveedores	S	S		S	S	S	S	S	S	S
Usuario Verificación Cartera	Recaudo y Transferencia							S			

Fuente: autores

ROLES, PROYECTOS Y PERMISOS MANTIS

La seguridad para el manejo de la información en MANTIS, se hace de la siguiente manera: A cada usuario se le asigna un rol y unos permisos dependiendo de los proyectos en el cual él participa (cuadro 11).

Cuadro 11. Proyectos MANTIS

Nombre	Descripción
Actualización y migración datos en las Bases de Datos	Los Jefes de Oficina y Vicepresidentes autorizarán los datos que será necesario actualizar o migrar a SIICOL
Base de datos Apuestas Deportivas Para mutuales	Base de datos APUESTAS DEPORTIVAS PARAMUTUALES
Base de Datos Baloto	Ambientes de bases de datos para BALOTO
Base de datos Superastro	Replica Base de datos Súper Astro COLJUEGOS
Charry	Proyecto Charry
Gestión Cuentas de Usuarios, Roles, Perfiles y Permisos	A través de este proyecto se solicita la gestión de cuentas de usuarios, tales como ingresos, retiros, vacaciones, etc. para las herramientas y aplicativos de COLJUEGOS. También se utiliza para asignar cuentas, roles y perfiles, a los diferentes sistemas de información y aplicaciones de Coljuegos.

Continuación Cuadro 11. Proyectos MANTIS

Nombre	Descripción
Gestión Incidentes de Seguridad de la Información	Se registrarán todas las acciones realizadas para solucionar los incidentes que sobre Seguridad de la Información que se presenten.
Ingreso de personal	Datos a incluir cuando una persona ingresa a Coljuegos
MET Desarrollo	Control en línea de las máquinas electrónicas tragamonedas
MET Producción	Control en línea MET
MET Pruebas	Control en Línea MET - Máquinas Electrónicas Tragamonedas
ORFEO-Desarrollo	Ambiente donde se realizan los nuevos desarrollos de Orfeo
Portal e Intranet	Proyecto nuevo portal e Intranet para Coljuegos
Promocionales	Este sub-proyecto corresponde a la modalidad de promocionales.
Proyecto ISOLUCION	Proyecto para estabilización del ambiente de pruebas de ISOLUCION
» Desarrollo ISOLUCION	Sub-proyecto ambiente de desarrollo ISOLUCIÓN
» Producción ISOLUCION	Sub-proyecto ambiente de producción ISOLUCIÓN
» Pruebas ISOLUCION	Sub-proyecto ambiente de pruebas ISOLUCIÓN
SARA	Proyecto correspondientes a los ambientes de producción y pruebas de la aplicación SARA
» Sara Producción	Ambiente de producción aplicación y base de datos SARA
» Sara Pruebas	Ambiente de pruebas para base de datos y aplicación SARA
SERVICIOS ADMINISTRATIVOS	Solicitud de Servicios Administrativos de COLJUEGOS
» Activos y Suministros	Solicitud Servicios de Activos y suministros.
Cuadro 11 (Continuación)	
» Adecuaciones Locativas	Solicitud de Adecuaciones Generales.

Continuación Cuadro 11. Proyectos MANTIS

Nombre	Descripción
» Mantenimientos Eléctricos	Solicitud de Servicios de Mantenimiento a la Infraestructura Eléctrica de COLJUEGOS.
» Servicios Generales	Solicitud de Servicios Generales.
SERVICIOS DE ARCHIVO Y CORRESPONDENCIA	Solicitud de servicios de archivo y correspondencia
» Servicios de Digitalización	Solicitud de Servicios de Digitalización
» Servicios de Estado de Envíos de Correspondencia	Solicitud del Estado de Envíos de Correspondencia
» Servicios de Fotocopiadoras e Impresoras	Solicitud de Servicios de Impresoras
» Servicios de ORFEO	Solicitud de servicios del sistema ORFEO
» Servicios de Prestamos Documentales y Consultas Digitales	Solicitud de Servicios para Prestamos Documentales
SIICOL Desarrollo	Proyecto Sistema de Información Integrado Coljuegos ambiente desarrollo
» Administración	Módulo para la administración de la aplicación SIICOL
» Base de Datos SIICOL	Base de datos SIICOL
» Cartera	Solicitudes sobre el módulo de cartera
» Cobro Coactivo	Solicitudes sobre el módulo de cobro coactivo
» Contabilidad	Solicitudes sobre el módulo de contabilidad
» Contratación administrativa	Solicitudes sobre el módulo de contratación administrativa
» Declaración y liquidación	Declaración y liquidación
» Distribución	Solicitudes sobre el módulo de distribución
» DME	Desarrollo de Mercado

Continuación Cuadro 11. Proyectos MANTIS

Nombre	Descripción
» GCT	Gestión Contractual
» Interfaces de usuario	Diseño de interfaces de usuario del proyecto SIICOL
» Migración	Solicitudes sobre el módulo de migración
» Nómina (SARA)	Solicitudes sobre el módulo de nómina
» PAC Y TESORERÍA	Solicitudes sobre el módulo de PAC y Tesorería
» Presupuesto	Solicitudes sobre el módulo de presupuesto
» Programación presupuestal	Solicitudes sobre el módulo de Programación presupuestal
» Recaudo	Solicitudes sobre el módulo de recaudo
» Transferencia	Solicitudes sobre el módulo de transferencia
SIICOL PRODUCCIÓN	Incidencias para SIICOL PRODUCCIÓN
Cuadro 11 (Continuación)	
SIICOL Test	Proyecto Sistema de Información Integrado Coljuegos ambiente de Test
» Base de Datos TEST SIICOL	Base de datos de prueba SIICOL
» Cartera Test	Solicitudes sobre el módulo de cartera (test)
» Cobro Coactivo Test	Solicitudes sobre el módulo de cobro coactivo (Test)
» Contabilidad Test	Solicitudes sobre el módulo de cobro contabilidad (Test)
» Declaración y liquidación Test	Declaración y liquidación Test
» Distribución Test	Solicitudes sobre el módulo de distribución(Test)
» DME Test	Desarrollo de Mercado Test
» GCT Test	Gestión Contractual Test
» Interfaces de Usuario Test	Interfaces de usuario Test

Continuación Cuadro 11. Proyectos MANTIS

Nombre	Descripción
» Migración Test	Solicitudes sobre el módulo de migración (Test)
» Nómina(SARA) Test	Solicitudes sobre el módulo de nómina (Test)
» PAC Y TESORERÍA Test	Solicitudes sobre el módulo de Pac y Tesorería (Test)
» Presupuesto Test	Solicitudes sobre el módulo de presupuesto(Test)
» Programación presupuestal Test	Programación presupuestal Test
» Recaudo Test	Solicitudes sobre el módulo de recaudo (Test)
» Transferencia Test	Solicitudes sobre el módulo de transferencia (Test)
SIITO Desarrollo	Este proyecto corresponde a SIITO.
SIITO Producción	Sistema Integrado de Información para trámites del operador.
SIITO Pruebas	Este sub-proyecto corresponde al proyecto SIITO pruebas de usuario
SIPLAFT Desarrollo	Proyecto Sistema Integral para la Prevención y Control del Lavado de Activos y Financiación del Terrorismo
SIPLAFT Producción	Sistema Integral para la Prevención y Control del Lavado de Activos y Financiación del Terrorismo
SIPLAFT Pruebas	Sistema Integral para la Prevención y Control del Lavado de Activos y Financiación del Terrorismo
Sistema SIVICAL	SIVICAL - Solución Informática para la Vigilancia, Inspección y Control de las apuestas en línea y tiempo real.
Soporte Técnico	Proyecto donde se colocan las diferentes solicitudes de soportes informáticos

Fuente: autores

Cuadro 12. Roles MANTIS.

Roles	Descripción del rol
Administrador	Es quien puede alterar todos los valores de configuración y es el usuario que tiene acceso a todos los niveles de acceso que mantis ofrece.
Manager	Posee todos los niveles de acceso que el desarrollador posee y puede actualizar incidencias de sólo lectura en cuanto al nivel de incidencias.
Desarrollador	En el nivel de acceso de incidencias este usuario puede reportar, actualizar, monitorizar, modificar, asignar, mover, borrar y reabrir incidencias, actualizar estado de las incidencias, ver incidencias privadas, definir visibilidad al añadir una nueva incidencia o nota, actualizar visibilidad de una incidencia o nota existente, ver lista de usuarios que monitorizan la incidencia. En cuanto al nivel de acceso a notas añade notas, actualizar notas, borrar nota, ver notas privadas de los demás. Y para otros accesos puede ver log de cambios, ver a quien fue asignada una incidencia y el Historial de la Incidencia y enviar recordatorios
Actualizador	En el nivel de acceso de incidencias este usuario puede reportar incidencia, actualizar incidencia, monitorizar incidencia, definir visibilidad al añadir una nueva incidencia o nota, actualizar visibilidad de una incidencia o nota existente. En cuanto al nivel de acceso a notas solo añade notas. Y para otros accesos puede ver log de cambios, ver a quien fue asignada una incidencia y el Historial de la Incidencia.
Informador	En el nivel de acceso de incidencias este usuario se le permite reportar Incidencia, monitorizar Incidencia, definir visibilidad al añadir una nueva incidencia o nota; en cuanto al nivel de acceso en notas estos piden añadir notas para otros accesos, puede ver log de cambios, ver a quien fue asignada una incidencia y el Historial de la Incidencia.
Espectador	Solo puede ver incidencias, y otros niveles de acceso como ver log de cambios, ver a quien fue asignada una incidencia y el historial de la incidencia

Fuente: autores

Cuadro 13. Permisos MANTIS.

Roles	Permisos							
	Mi Vista	Ver incidencias	Reportar incidencia	Registro de cambios	Roadmap	Resumen	Administración	Mi cuenta
Administrador	X	X	X	X	X	X	X	X
Manager	X	X	X	X	X			X
Desarrollador	X	X	X	X	X			X
Actualizador	X	X	X	X	X			X
Informador	X	X	X					
Espectador	X	X		X				X

Fuente: autores

ROLES, MÓDULOS Y PERMISOS SIPLAFT

La seguridad para el manejo de la información en SIPLAFT, se hace de la siguiente manera: Primero al funcionario se le asigna uno de los siguientes roles mostrados en el cuadro de roles (cuadro 14) y posteriormente se le asigna los permisos que se consideren y que se encuentran definidos en el cuadro de permisos (cuadro 15).

Cuadro 14. Roles SIPLAFT

Rol	Descripción del rol
Administradores	Administra los usuarios y claves de la aplicación
Operadores	Operadores SIPLAFT

Fuente: autores

Cuadro 15. Permisos SIPLAFT.

Rol	Descripción del rol	Permisos											
		Administración usuarios				Cargue formularios				Consulta acuses de recibo			
		Ingresar	Consultar	Modificar	Borrar	Ingresar	Consultar	Modificar	Borrar	Ingresar	Consultar	Modificar	Borrar
Administradores	Administra los usuarios y claves de la aplicación	X	X	X	X						X		
Operadores	Operadores SIPLAFT					X	X	X	X		X		

Fuente: autores

ROLES, MÓDULOS Y PERMISOS MET-SCLM

La seguridad para el manejo de la información en MET-SCLM, se hace de la siguiente manera: Primero al funcionario se le asigna uno de los siguientes roles mostrados en el cuadro de roles (cuadro 16) y posteriormente se le asigna los permisos que se consideren y que se encuentran definidos en el cuadro de permisos (cuadro 17).

Cuadro 16. Roles MET-SCLM

Roles	Descripción de roles
Administrador	Administra los usuarios y claves de la aplicación
Operador	Operador de juegos de suerte y azar validado y autorizado por COLJUEGOS
Coordinador SAC	Coordinador Servicio al Cliente, asigna las solicitudes a los analistas
Coordinador DME	Coordinador Gerencia Negocios Actuales, asigna las solicitudes a los analistas
Coordinador GAF	Coordinador Gerencia Administrativa y Financiera, asigna las solicitudes a los analistas
Analista SAC	Analista SAC, verifica, aprueba o rechaza las solicitudes
Analista DME	Analista GNA, valida, aprueba o rechaza las solicitudes
Analista GAF	Analista GAF, valida, aprueba o rechaza las solicitudes
Analista calidad DME	Analista GAF, valida, aprueba o rechaza las solicitudes

Fuente: autores

Cuadro 17. Permisos MET.SCLM.

Roles	Descripción de roles	Administra ción usuarios	Diligencia miento y Cargue formulario s	Asignar Analista	Verificar, validar, aprobar, rechazar, Solicitud	Desistir solicitud	Generar requerí miento	Responder requerimien to
ADMINISTRADOR	Administra los usuarios y claves de la aplicación	X						
OPERADOR	Operador de juegos de suerte y azar validado y autorizado por COLJUEGOS		X			X		X
COORDINADOR SAC	Coordinador Servicio al Cliente, asigna las solicitudes a los analistas			X				
COORDINADOR DME	Coordinador Gerencia Negocios Actuales, asigna las solicitudes a los analistas			X				
COORDINADOR GAF	Coordinador Gerencia Administrativa y Financiera, asigna las solicitudes a los analistas			X				
ANALISTA SAC	Analista SAC, verifica, aprueba o rechaza las solicitudes				X		X	
ANALISTA DME	Analista GNA, valida, aprueba o rechaza las solicitudes				X		X	
ANALISTA GAF	Analista GAF, valida, aprueba o rechaza las solicitudes				X		X	
ANALISTA CALIDAD DME	Analista GAF, valida, aprueba o rechaza las solicitudes				X		X	

Fuente: autores

ROLES, MÓDULOS Y PERMISOS SIITO

La seguridad para el manejo de la información en SIITO, se hace de la siguiente manera: Primero al funcionario se le asigna uno de los siguientes roles mostrados en el cuadro de roles (cuadro 18) y posteriormente se le asigna los permisos que se consideren y que se encuentran definidos en el cuadro de permisos (cuadro 19).

Cuadro 18. Roles SIITO

Roles	Descripción de roles
ADMINISTRADOR	Administra los usuarios y claves de la aplicación
OPERADOR	Operador de juegos de suerte y azar validado y autorizado por COLJUEGOS
COORDINADOR SAC	Coordinador Servicio al Cliente, asigna las solicitudes a los analistas
COORDINADOR DME	Coordinador Gerencia Negocios Actuales, asigna las solicitudes a los analistas
COORDINADOR GAF	Coordinador Gerencia Administrativa y Financiera, asigna las solicitudes a los analistas
ANALISTA SAC	Analista SAC, verifica, aprueba o rechaza las solicitudes
ANALISTA DME	Analista GNA, valida, aprueba o rechaza las solicitudes
ANALISTA GAF	Analista GAF, valida, aprueba o rechaza las solicitudes
ANALISTA CALIDAD DME	Analista GAF, valida, aprueba o rechaza las solicitudes

Fuente: autores

Cuadro 19. Permisos SIITO

Roles	Descripción de roles	Administración usuarios	Diligenciamiento y Cargue formularios	Asignar Analista	Verificar, validar, aprobar, rechazar, Solicitud	Desistir solicitud	Generar requerimiento	Responder requerimiento
ADMINISTRADOR	Administra los usuarios y claves de la aplicación	X						
OPERADOR	Operador de juegos de suerte y azar validado y autorizado por COLJUEGOS		X			X		X
COORDINADOR SAC	Coordinador Servicio al Cliente, asigna las solicitudes a los analistas			X				
COORDINADOR DME	Coordinador Gerencia Negocios Actuales, asigna las solicitudes a los analistas			X				
COORDINADOR GAF	Coordinador Gerencia Administrativa y Financiera, asigna las solicitudes a los analistas			X				
ANALISTA SAC	Analista SAC, verifica, aprueba o rechaza las solicitudes				X		X	
ANALISTA DME	Analista GNA, valida, aprueba o rechaza las solicitudes				X		X	
ANALISTA GAF	Analista GAF, valida, aprueba o rechaza las solicitudes				X		X	
ANALISTA CALIDAD DME	Analista GAF, valida, aprueba o rechaza las solicitudes				X		X	

Fuente: autores